Network-based IP flow mobility Support in 3GPPs Evolved Packet Core

Prepared by:

Charna Tina John

Supervised by:

Neco Ventura

This thesis is submitted in fulfillment of the academic requirements
for the degree of
Master of Science in Electrical Engineering
in the Faculty of Engineering and The Built Environment
University of Cape Town
November 2013

As the candidate‟s supervisor, I have approved this dissertation for submission.

Name: Neco Ventura

Signed: _____

Date: _____

Declaration

I hereby declare that: (1) the above thesis is my own unaided work, both in conception and execution, and that apart from the normal guidance of my supervisor, I have received no assistance apart from that stated below; (2) except as stated below, neither the substance or any part of the thesis has been submitted in the past, or is being, or is to be submitted for a degree in the University or any other University.

I am now presenting the thesis for examination for the Degree of Master of Science in Electrical Engineering. I also grant the University free license to reproduce the above thesis in whole or in part, for the purpose of research.

Charna Tina John

Name

Date

Acknowledgements

I would like to acknowledge and extend my deepest gratitude to the following individuals and organisations for their guidance and assistance during the course of this project:

- My parents, for their comprehensive support, love and for always believing in me.
- Mr. Neco Ventura my supervisor, for his time, encouragement, advice and guidance throughout the time I have been his student.
- Telkom SA and the Centre of Excellence for funding my Master"s studies.
- Sibonelo Madlopha, Joseph Orimolade and Joyce Mwangama, for providing me with the support and the friendship I needed, and for sharing their knowledge and constant encouragement throughout the past three years.

Abstract

Mobile data traffic in cellular networks has increased tremendously in the last few years. Due to the costs associated with licensed spectrum, Mobile Network Operators (MNOs) are battling to manage these increased traffic growths. Offloading mobile data traffic to alternative low cost access networks like Wi-Fi has been proposed as a candidate solution to enable MNOs to alleviate congestion from the cellular networks. This dissertation investigates an offloading technique called IP flow mobility within the 3rd Generation Partnership Project (3GPP) all-IP mobile core network, the Evolved Packet Core (EPC). IP flow mobility would enable offloading a subset of the mobile user‟s traffic to an alternative access network while allowing the rest of the end-user‟s traffic to be kept in the cellular access; this way, traffic with stringent quality of service requirements like Voice over Internet Protocol (VoIP) would not experience service disruption or interruption when offloaded. This technique is different from previous offloading techniques where all the end-user‟s traffic is offloaded.

IP flow mobility functionality can be realised with either host- or network-based mobility protocols. The recommended IP flow mobility standard of 3GPP is based on the host-based mobility solution, Dual-Stack Mobile IPv6. However, host-based mobility solutions have drawbacks like long handover latencies and produce signaling overhead in the radio access networks, which could be less appealing to MNOs. Network-based mobility solutions, compared to the host-based mobility solutions, have reduced handover latencies with no signaling overhead occurring in the radio access network. Proxy Mobile IPv6 is a network-based mobility protocol adapted by 3GPP for mobility in the EPC. However, the standardisation of the Proxy Mobile IPv6-based IP flow mobility functionality is still ongoing within 3GPP. A review of related literature and standardisation efforts reveals shortcomings with the Proxy Mobile IPv6 mobility protocol in supporting IP flow mobility. Proxy Mobile IPv6 does not have a mechanism that would ensure session continuity during IP flow handoffs or a mechanism enabling controlling of the forwarding path of a particular IP flow i.e., specifying the access network for the IP flow. The latter mechanism is referred to as IP flow information management and flow-based routing. These mechanisms represent the basis for enabling the IP flow mobility functionality.

To address the shortcomings of Proxy Mobile IPv6, this dissertation proposes

enhancements to the protocol procedures to enable the two mechanisms for IP flow mobility functionality. The proposed enhancements for the session continuity mechanism draw on work in related literature and the proposed enhancements for the IP flow information management and flow-based routing mechanism are based on the concepts used in the Dual-Stack Mobile IPv6 IP flow mobility functionality. Together the two mechanisms allow the end-user to issue requests on what access network a particular IP flow should be routed, and ensure that the IP flows are moved to the particular access network without session discontinuity.

The proposed IP flow mobility functionality is implemented in a standards compliant real emulated EPC testbed. The testbed is used for demonstrating proof of concept and to evaluate the proposed IP flow mobility functionality. To evaluate the proposed IP flow mobility functionality, tests were conducted to determine whether the solution performs within established criteria and whether the overheads introduced by the solution would have an acceptable effect on the end-user experience. The performance metrics used for the evaluation were IP flow handover latency, signaling overhead, packet processing delay and throughput. It has been found that the IP flow handover latency falls within the established criteria and while there is a cost in signaling overhead, packet processing delay and throughput, this cost will have an acceptable effect on the end-user experience.

Table of Contents

List of Figures

List of Tables

List of Acronyms

3GPP	Third Generation Partnership Project
AAA	Access Authentication and Authorization
AA-A	AA-Answer
AAR	AA-Request
ANDSF	Access Network Discovery and Selection Function
APN	Access Point Name
ATT	Access Technology Type
BA	Binding Acknowledge
BBERF	Bearer Binding and Event Reporting Function
BC	Binding Cache
BCE	Binding Cache Entry
BID	Binding Identification
bps	Bits per second
BU	Binding Update
BUL	Binding Update List
BULE	Binding Update List Entry
CDMA2000	Code Division Multiple Access 2000
CoA	Care-of Address
CPS	Calls per Second
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DSMIPv6	Dual Stack Mobile Internet Protocol version 6
EHCP	Enhanced Host Configuration Protocol
EPC	Evolved Packet Core
ePDG	evolved Packet Data Gateway
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FBC	Flow Binding Cache
FBE	Flow Binding Entry
FBL	Flow Binding List
FID	Flow Identification
FID-PRI	Flow Identification Priority
FMA	Flow Mobility Acknowledge
FMI	Flow Mobility Initiate
FMI	Flow Mobility Indicate
FTP	File Transfer Protocol
GPL	General Public License

GPRS	General Packet Radio Service
GTP	GPRS Tunnelling Protocol
GTP-C	GPRS Tunnelling Protocol Control-Plane
GTP-U	GPRS Tunnelling Protocol User-Plane
GUI	Graphical User Interface
HA	Home Agent
HNP	Home Network Prefix
HoA	Home Address
HSPA	High Speed Packet Access
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
HUA	Home Network Prefix Update Acknowledge
HUR	Home Network Prefix Update Request
Hz	Hertz
ID	Identity
IETF	Internet Engineering Task Force
IFOM	IP Flow Mobility
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPCAN	Internet Protocol Connectivity Access Network
IPTV	Internet Protocol Television
IPv6	Internet Protocol version 6
Kb	Kilobits
Kbps	Kilobits per second
KPI	Key Performance Indicator
LIF	Logical Interface
LMA	Local Mobility Anchor
LTE	Long Term Evolution
LTS	long Term Solution
MAC	Medium Access Control
MAG	Mobile Access Gateway
MB	Mega Byte
Mbps	Mega bits per second
MDF	Media Delivery Function
MH	Mobility Header
MHz	Mega Hertz
MIP	Mobile Internet Protocol
MIPv6	Mobile Internet Protocol version 6
MM	Mobility Manager
MME	Mobility Management Entity
MNO	Mobile Network Operator

myMONSTER	Multimedia Open InterNet Services and Telecommunication EnviRonmen
NIF	New Interface
nMAG	new Mobile Access Gateway
NS-3	Network Simulator version 3
OS	Operating System
p2p	peer-to-peer
PBA	Proxy Binding Acknowledge
PBU	Proxy Binding Update
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
P-CoA	Proxy Care-of Address
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDN-GW	Packet Data Network Gateway
PIF	Previous Interface
PMIPv6	Proxy Mobile Internet Protocol version 6
QoE	Quality of Experience
QoS	Quality of Service
RAM	Random Access Memory
RAN	Radio Access Network
RFC	Request for Comments
RTT	Round Trip Time
SAE	Systems Architecture Evolution
SDP	Session Description Protocol
S-GW	Serving Gateway
SIP	Session Initiation Protocol
STA	Session Termination Answer
STR	Session Termination Request
TCP	Transmission Control Protocol
UCT	University of Cape Town
UDP	User Datagram Protocol
UE	User Equipment
UE-ID	User Equipment Identity
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
VNI	Visual Networking Index
VoD	Video on Demand
VoIP	Voice over Internet Protocol
WCDMA	Wideband Code Division Multiple Access
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

Chapter 1

Introduction

In the last few years, Mobile Network Operators (MNOs) have experienced tremendous data explosion on their cellular networks. This is mainly attributed to the increasing number of wireless subscribers accessing mobile data services that are partially due to:

- The proliferation of data hungry mobile devices such as tablets, smartphones (iPhone, Blackberry, Android phone) and laptops.
- MNOs offering cost-effective mobile broadband services based on USB modems and data cards.
- The availability of a plethora of bandwidth intensive mobile applications such as YouTube, mobile Internet Protocol Television (IPTV) and Skype.

These developments will continue to drive the increase in mobile data traffic and are creating challenges for MNOs in supporting these traffic growths, especially since licensed spectrum is limited [1]. An expected development that could solve this issue for MNOs is with the introduction of the 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS) [2]. The EPS meets two objectives: Firstly, it defines the Long Term Evolution (LTE) [3] macro Radio Access Network (RAN). LTE is currently the most advanced and widely embraced RAN and boasts characteristics such as, having the possibility of providing downlink peak rates of 300 Mega bits per second (Mbps) and uplink peak rates of 75 Mbps, ensuring data transfer latencies of less than 5ms in the RAN and providing increased spectral efficiency (16.32 bits per Hertz (Hz) per mobile) [3]. The second objective of the EPS is to define the core network of LTE, the Evolved Packet Core (EPC) [2]. The EPC was a result of the 3GPP Systems Architecture Evolution (SAE) work item, whose main goal was to evolve

the packet core networks defined by 3GPP (e.g. Universal Mobile Telecommunications System (UMTS)) to create an all-IP packet core network that is not just the core for LTE, but allowing interworking of multiple RANs which includes 3GPP RANs such as General Packet Radio Service (GPRS), Wideband Code Division Multiple Access (WCDMA) and High Speed Packet Access (HSPA), as well as non-3GPP [4] RANs such as Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WiMAX) and Code Division Multiple Access 2000 (CDMA2000). The work item also provides a common set of tools that network operators can utilise for mobility, charging, Quality of Service (QoS) and security.

The introduction of the EPC and LTE will enable operators to provide data services at a much lower operational cost. For example, the current cost levels for HSPA+ in the USA is around $0.01 per-Mega Byte (per-MB), and with the introduction of LTE, these costs are expected to decrease by a factor of 10 (i.e. $0.001per-MB) [5]. With this significant cost reduction, mobile data traffic is expected to increase even further. This is evident from the findings on the trends and predictions in internet traffic of the Cisco Visual Networking Index (VNI) [6]. The Cisco VNI is an ongoing initiative to track and forecast the impact of visual networking applications on service providers [6]. From the findings, it is expected that the overall mobile data traffic will grow to 10.8 exabytes per month by the year 2016, which is an 18-fold increase from the year 2011 [6] that was merely 0.8 exabytes per month. Thus, the introduction of LTE will not be enough for surpassing the forecasted mobile traffic growth.

To cope with the expected increasing traffic growth, MNOs may use traditional methods to increase network capacity e.g. deploying more LTE base stations. But this method entails high cost investments which leaves the MNOs seeking other alternatives to increase network capacity. In this regard, MNOs are investigating intelligent traffic management solutions. One such solution that has been gaining interests from MNOs is seamless and intelligent offloading of mobile data traffic via complementary access networks. Operators have identified two possible complementary access networks for their offloading solutions: LTE femtocells and WLAN. LTE femtocells are small base stations that are installed inside homes or buildings and were brought on by the need to improve signal-strength in these restricted areas [7]. Using LTE femtocells is a viable approach, but wide spread deployment has not been realised thus far. This is due to the operational challenges of deploying and supporting them. For example, LTE femtocells operate in the same frequency bands as the LTE macrocells which means that there is bound to be interference generated between the radio signals. Hence, enabling MNOs to install femtocells successfully requires intelligent

mechanisms for preventing interference between LTE femtocells and LTE macrocells. WLAN, on the other hand, is more appealing at this stage, since it uses unlicensed radio spectrum (which means there is no radio interference with LTE macrocells), is widely deployed in both residential and corporate environments (e.g. schools, houses, hospitals, universities, etc.) and since a Wi-Fi interface is present in all new smartphones, tablets, laptops and other consumer electronics.

WLAN offloading solutions for the EPC have been evolving within the 3GPP standardization body. This is since the EPC is the current promising core network solution to combat the effect of the current and future increasing mobile data traffic, and since 3GPP has defined the EPC with WLAN access integration from the beginning of their release 8 [2] standards. At the outset it becomes clear that the mobility management solution that the EPC employs for handoffs between 3GPP accesses and WLAN accesses are important, as each has relevance in the type of offloading scenarios operators can realise, and plays a vital role in the type of experience the end-users receive from the offloading solution. There are two types of WLAN offloading scenarios that can be realised in the EPC: In the first scenario, whenever the User Equipment (UE) is under the coverage of a WLAN access the entire IP traffic of the user will be offloaded to WLAN. This was the only scenario possible with the release 8 mobility management solution of the EPC. 3GPP soon realised that this approach would greatly affect end-user quality of experience since all the IP traffic of the end-user is offloaded to WLAN while traffic like VoIP, with stringent Quality of Service (QoS) requirements in terms of handover latencies, will experience service disruption or interruption. Thus, to improve the flexibility of the WLAN mobility management solution, 3GPP in release 10 standardised an extension to the mobility management solution, called IP flow mobility [8], which allows the UE to simultaneously connect to a macro access network (e.g. LTE) and a WLAN access, and allowing a subset of the UE's traffic to be moved on a per-IP-flow basis between the accesses. For example, moving a File Transfer Protocol (FTP) file to WLAN while, at the same time, keeping the rest of the traffic on the macro network (e.g. Voice over Internet Protocol (VoIP) on LTE). Hence, in the second WLAN offloading scenario, when the UE is under the coverage of a WLAN access, only a subset of the end-users traffic could be offloaded to WLAN. Figure 1.1 illustrates an example use case scenario of WLAN offloading with IP flow mobility. In Figure 1.1.a, the UE is connected to LTE and have two IP flows, a VoIP IP flow and a non-conversational video IP flow. The UE then moves into an overlapping LTE/WLAN coverage area (Figure 1.1.b) and based on operator defined policies (e.g. non-conversational video should be offloaded to WLAN), user

preferences (e.g. cost) or application requirements (e.g. bandwidth), the non-conversational video IP flow is offloaded to WLAN. In this document an IP flow is defined as a stream of packets matching a particular packet descriptor [9]. An example packet descriptor is the IP 5-tuple of an IP packet, comprising of the source and destination IP addresses, source and destination port numbers and transport layer protocol (e.g. Transmission Control Protocol (TCP), User Datagram Protocol (UDP), etc.).

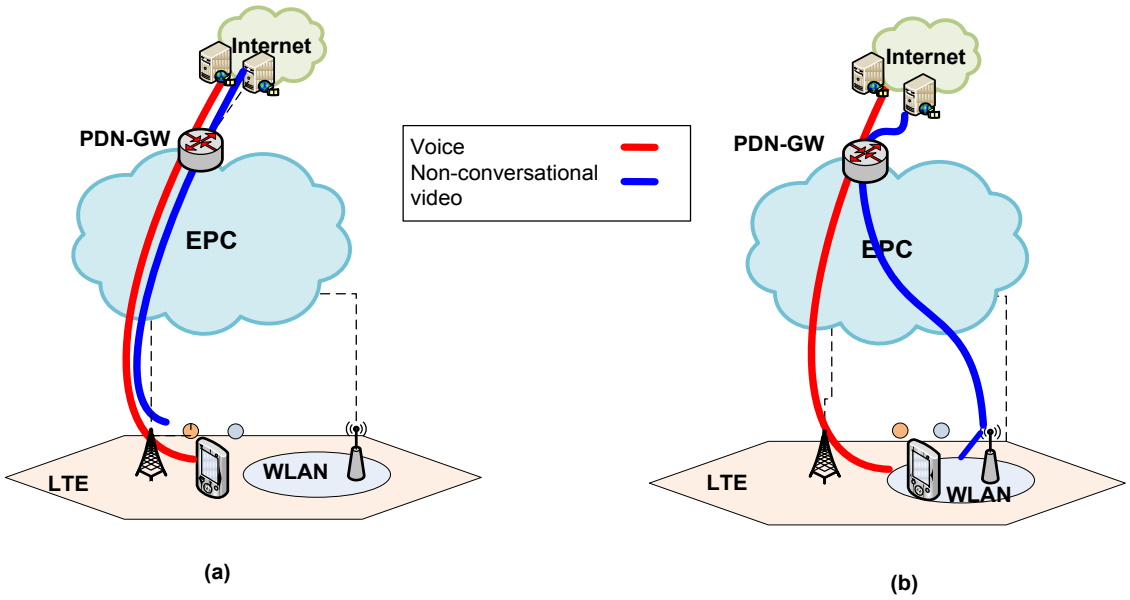

Figure 1.1: WLAN offloading via IP flow mobility in the EPC

IP flow mobility is an attractive mobility solution to operators since in addition to offering offloading capabilities it creates opportunities for new functionalities such as:

- Enabling policy based routing where the operators can set policies in the network for effectively steering traffic over the available RANs. For example, an operator can define a policy to offload only traffic with less stringent QoS requirements like FTP to WLAN, while keeping traffic (e.g. VoIP) with stringent QoS requirements on the cellular networks where robust QoS support mechanisms exist.
- Load-sharing by spreading the network traffic load among several routes.
- Bandwidth aggregation: splitting an IP flow amongst several available UE interfaces or routes with the intention of increasing the bandwidth of that IP flow.
- Operators can offer seamless handovers by offering make-before-break type handovers to end-users with new generation mobile devices. Devices nowadays come equipped with multiple network interfaces like GPRS, WCDMA/HSPA, LTE, Bluetooth and WLAN, with some having the capability to send and receive data using

multiple interfaces simultaneously (for instance using WLAN and HSPA or WLAN and LTE). This is due to that the difference in power levels and frequency bands of these RANs which means no interference is generated between the radios [10].

These are but a few of the benefits of IP flow mobility, the list is expandable.

WLAN offloading solutions via IP flow mobility in the EPC requires various components, each contributing to create a complete solution for MNOs. These components include: Policy and Charging Control (PCC) [11] for QoS and charging of the individual IP flows, Access Authentication and Authorization (AAA) to provide security for end-users through WLAN, and the IP flow mobility management solution itself [8] providing the actual functionality to route traffic on an IP flow level and ensuring session continuity between the access networks when an IP flow is offloaded. The components mentioned all constitute different working items within 3GPP and are specified separately. A complete WLAN offloading solution via IP flow mobility is thus complex; hence this research addresses only the IP flow mobility, mobility management solution for realising WLAN offload in EPC. The mobility management solution constitutes the base component of the complete IP flow mobility solution.

1.1 Problem description

IP flow mobility can be realised with either host- or network-based mobility management solutions. Host-based refer to mobility management solutions requiring special functionality in the UE to orchestrate mobility signalling towards a mobility agent within the core network. Network-based mobility management solutions rely on the network for the agent functionality and for orchestrating the mobility signalling on behalf of the UE. With network-based mobility management solutions, the mobility functionalities within the network are transparent from the UE and therefore simpler to implement.

Host-based mobility management solutions in general have not been widely deployed due to the poor network performance incurred through their use. For instance, research studies [12] [13] have shown that these solutions suffer from long handover latencies, high packet loss rates and produce signaling overhead in the RANs of the operators‟ network. Conversely, comparing the performance of network-based mobility management solutions with that produced by host-based solutions, it is shown that the handover latency and packet lost rates are significantly reduced with no signaling overhead occurring in the RAN. This is evident from similar studies [14] [15] [16] conducted in the literature.

The currently standardised IP flow mobility solution by 3GPP is based on an Internet Engineering Task Force (IETF) standardised mobility protocol, Dual Stack Mobile Internet Protocol version 6 (DSMIPv6) [17]. DSMIPv6 is classified as a host-based mobility management solution and due to the drawbacks of these solutions, MNOs find this IP flow mobility solution less appealing and are seeking IP flow mobility solutions based on network-based mobility management solutions instead. IETF standardised a mobility protocol, called Proxy Mobile Internet Protocol version 6 (PMIPv6) [18] and is classified as a network-based mobility management solution, and is one of the mobility protocols adopted by 3GPP for mobility [4] [19] between 3GPP accesses and non-3GPP accesses in the EPC. 3GPP is also investigating the use of the PMIPv6 protocol for providing IP flow mobility capabilities in the EPC [8]. However, the standardisation of the PMIPv6-based IP flow mobility solution is still ongoing which makes the design of such a solution a present and attractive research area.

Due to the benefits of network-based mobility management solutions, further investigation is thus required on developing a network-based IP flow mobility solution with the PMIPv6 protocol for 3GPPs EPC. Developing an IP flow mobility solution for the EPC would allow MNOs to combat the expected mobile traffic growth by utilising the IP flow mobility solution for offloading traffic to WLAN access networks, and would allow MNOs to enhance the capabilities and performance of the EPC by taking advantage of the benefits an IP flow mobility solution offers. PMIPv6-based IP flow mobility solutions have been proposed in related works [9] [20] [21] [22] [23], but these proposals do not consider PMIPv6 in relation to the EPC, especially with how the protocol integrates into the EPC network and how it has been adapted by 3GPP for enabling mobility for the end-users. Related work regarding IP flow mobility support in the EPC is thus lacking. Hence, developing an IP flow mobility solution for the EPC would greatly contribute to the area of IP flow mobility research currently ongoing in the research community and the 3GPP standardisation body.

1.2 Thesis objectives

The main goal of this research is on the analysis, design and implementation of a PMIPv6-based IP flow mobility solution for 3GPPs Evolved Packet Core. The solution would enable mobile network operators to offload mobile data traffic to WLAN while augmenting the end-user‟s quality of experience. The thesis objectives can be summarised as follows:

1. Review the EPC network and the PMIPv6-based IP flow mobility solution currently undergoing standardisation within 3GPP to identify the requirements and functional

components in the EPC to support WLAN access networks and PMIPv6-based IP flow mobility.

2. Review the available PMIPv6-based IP flow mobility proposals in the literature and the key components proposed by other standardisation bodies to determine how it is affecting the developing PMIPv6-based IP flow mobility standard in 3GPP and to identify the missing gaps from the 3GPP proposed PMIPv6 IP flow mobility solution.

3. Propose a PMIPv6-based IP flow mobility solution for the EPC to achieve WLAN offloading. The goal of this solution is to extract useful concepts from related works and build on and fill in the missing gaps identified in 3GPPs proposed solution. These missing gaps constitutes: the functionality to ensure session continuity during IP flow handoffs between the interfaces of the end-user‟s device while being multihomed (i.e., the ability of an end-user‟s device to simultaneously attach multiple interfaces to the EPC and transmit/receive data on these multiple interfaces), and the functionality to enable the controlling and redirecting IP flow between the access networks the end-user is attach to.

4. Develop a prototype implementation of the proposed PMIPv6-based IP flow mobility solution on a real testbed environment: the FOKUS OpenEPC [24] testbed. The prototype implementation is used to analyse the effectiveness of the proposed solution in performing IP flow mobility and to perform testing and evaluation of the impacts the IP flow mobility solution has on the EPC network and the end-user experience.

5. Give an analysis of the impact the proposed IP flow mobility solution has on the EPC network and the end-user based on the results obtained from the testbed prototype implementation. In particular, results from proof of concept tests and performance tests are evaluated. The goals of the proof of concept tests are to validate the proposed IP flow mobility functionality and to show that IP flow mobility functionality could enhance the end-user quality of experience compared to the scenario resulting in the complete offloading of the end-users traffic. The goal of the performance tests is to evaluate the effect IP flow mobility functionality could have on the EPC network performance. The performance metrics measured in the proof of concept tests are those that would indicate the validity of the proposed IP flow mobility functionality, which is throughput, and those that would indicate the performance of the end-user IP flows; these are packet loss and goodput. The performance metrics measured in the performance tests are packet processing delay, throughput, signaling overhead and IP

flow handover latency. These metrics are used to determine how the proposed IP flow mobility functionality performs.

1.3 Scope and limitations

Mobility management solutions can be applied at different layers of the protocol stack. This means the area of mobility management is very broad. Discussions on the mobility solutions beyond the network-layer are outside the scope of this project. This research only focuses on the PMIPv6 mobility solution supported in the EPC, and only related work with the most relevance to IP flow mobility will be addressed in this research.

In this research, only mobility within a local administrative domain is considered which means the scenario where the UE is simultaneously attached to different administrative domains (and possibly administered by different MNOs) is not addressed in this research.

The research is restricted to a single mobility agent functionality of the PMIPv6 protocol. This means that the issue of the mobility signaling arriving at the wrong mobility agent are ignored, and the UE can only be simultaneously connected to the EPC with one 3GPP and only one non-3GPP RAN and cannot have multiple simultaneous connections to the same RAN.

Intelligent decision mechanisms within the UE or network to initialise the IP flow mobility procedures are outside the scope of this research. For example, the decision to initiate IP flow mobility procedures is not triggered by service characteristics (e.g. QoS requirements) or the state of the available RANs (e.g. congestion) or even the UE discovering a new RAN, instead the trigger is manually initiated for flow handoff.

1.4 Contributions

The contributions of this dissertation include:

- Design of PMIPv6-based IP flow mobility functionality for 3GPPs Evolved Packet Core. The design includes a mechanism to support session continuity during IP flow handoffs for multihomed end-user devices. The design also includes a mechanism to support IP flow information management and flow-based routing. This mechanism enables the end-user to indicate to the network how a particular IP flow should be routed, and allows the network to manage IP flow mobility information on a per end-

user basis. Both mechanisms entail enhancements to the PMIPv6 mobility protocol procedures and signaling messages, as well as the end-user device.

- The proof of concept testbed implementation of the proposed IP flow mobility functionality is developed with the OpenEPC [24] software toolkit of Fraunhofer FOKUS. The software toolkit is compliant with the 3GPP standards and provides all the entities of 3GPPs EPC architecture and an implementation of the PMIPv6 mobility solution. However, the toolkit does neither support end-users attaching with multiple interfaces simultaneously nor does it have any of the required IP flow mobility mechanisms. Another contribution of this research is the extensions that had been made to the OpenEPC toolkit to support the proposed IP flow mobility design.

The contributions of this MSc research are documented in the following publications:

1. **C. John** and N. Ventura, "Design of IP flow mobility functionality for a PMIPv6-based Evolved Packet Core", *Proceedings of 2012 16th Southern African Telecommunications Network and Applications Conference (SATNAC'13),* September 2013.

2. **C. John**, S. Madlopha and N. Ventura, "PMIPv6-based Make-before-break Handover for Real-time Services in 3GPPs Evolved Packet Core", *Proceedings of the IEEE 2013 International Conference on Information Networking (ICOIN 2013)*, Bangkok, Thailand, 28-30 January, 2013.

3. **C. John** and N. Ventura, "Service Continuity in Network-based IP Flow Mobility in the Evolved Packet Core", *Proceedings of 2012 15th Southern African Telecommunications Network and Applications Conference (SATNAC'12)*, September 2012. [The publication received the best-paper award]

4. **C. John** and N. Ventura, "WLAN Offload and IP Flow Mobility in the Evolved Packet Core", *Proceedings of 2011 14th Southern African Telecommunications Network and Applications Conference (SATNAC'11)*, September 2011.

1.5 Thesis Outline

The remainder of the dissertation is structured as follows:

Chapter 2 presents an overview of the EPC and discusses the components for allowing the interworking of WLAN accesses. This is followed by an overview of the PMIPv6 mobility solution and outlines the required architecture within the EPC. A discussion of the

PMIPv6-based IP flow mobility solution of 3GPP is then given, highlighting the key components proposed by the IETF standardisation body, and how it is affecting the finalisation of the PMIPv6-based IP flow mobility solution by 3GPP. An investigation and review is then given on the PMIPv6-based IP flow mobility proposals available in the literature, focussing on their contributions and limitations to determine the key components still missing from the 3GPP IP flow mobility proposal and that would aid in the design of the PMIPv6 IP flow mobility solution in the EPC.

Chapter 3 discusses the requirements and functionality identified for enabling IP flow mobility functionality in the EPC. In particular, the protocol and architectural requirements are discussed. Followed by a description of the proposed PMIPv6-based IP flow mobility solution for the EPC architecture and the IP flow mobility scenarios that the proposed solution can achieve.

Chapter 4 is devoted to a description of the configuration and design of the prototype on the FOKUS OpenEPC testbed. It also discusses the drawbacks, limitations as well as the tools and equipment used for the prototype implementation.

In **Chapter 5** the prototype implementation and proposed IP flow mobility mechanisms are subjected to validation tests and performance tests and the results presented. The tests aim to demonstrate proof of concept and evaluate the effectiveness of the proposed IP flow mobility functionality.

Chapter 6 presents the conclusions obtained from this research and gives recommendations for further research relating to IP flow mobility.

Chapter 2

Literature Review

The 3GPP standardisation body [25] has defined data offloading via alternate low-cost access networks (e.g. WLAN) as a key solution for enabling MNOs to manage the excepted traffic growth on the EPS. WLAN offloading solutions has been a critical area of study in 3GPP Release-10 and to this end, 3GPP standardised a WLAN offloading solution for the EPC called IP flow mobility [8], where some of the user data is selectively re-directed from an access network (while simultaneously leaving the rest of the user data in the source network) and thus avoiding overload and improving the end-user Quality of Experience (QoE). The IP flow mobility solution is based on the EPC, as it allow interworking non-3GPP RANs such as WLAN. The standard IP flow mobility solution is based on the Dual Stack Mobile IP version 6 (DSMIPv6) mobility protocol. However, MNOs find this solution less appealing since DSMIPv6 has many disadvantages (e.g. induces signaling overhead in the RAN and requires software enhancements on the UE); they are instead seeking IP flow mobility solutions based on network-based mobility protocols. Proxy Mobile IPv6 (PMIPv6), a network-based mobility protocol providing inter-system mobility in the EPC is one of the candidate mobility protocols currently being investigated by 3GPP for IP flow mobility. However, 3GPP has not yet standardised the PMIPv6-based IP flow mobility solution. A technical report produced by 3GPP on Network-based IP flow mobility [26] proposes that the mechanisms enabling IP flow mobility for DSMIPv6 be applied to PMIPv6 for enabling IP flow mobility. These mechanisms include a mechanism enabling multiple interface connectivity and session continuity during IP flow handoff, and a mechanism enabling flow-based routing and

allowing the UE to set forwarding preferences for the IP flows in the network (these mechanisms will be discussed in this chapter). However, when considering PMIPv6 the mechanisms cannot be applied to the protocol since the standard procedures for IP allocation, binding cache managements and due to the lack of_UE intervention in the processing and orchestration of mobility signalling are different to that of DSMIPv6. These issues are discussed in this chapter.

This chapter starts by presenting background information on relevant concepts for the purpose of grasping the mechanisms that enable IP flow mobility in the EPC. The standardised DSMIPv6-based IP flow mobility solution will then be reviewed since it impacts the efforts towards the standardisation of the PMIPv6 IP flow mobility solution by 3GPP, and will introduce the technical mechanisms of an IP flow mobility solution. Related works on PMIPv6-based IP flow mobility solutions are then reviewed in terms of how they solve the session continuity and flow-based routing and management issues, and the limitations associated to them.

2.1 Background Information

2.1.1 3GPP EPC architecture

The EPS [2] comprises of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) [3], also known as LTE, and the E-UTRAN core network: the EPC. E-UTRAN is the RAN providing the communication between the UE and the EPC and achieves this communication using base stations known as eNodeB. The EPC is a flat all-IP packet switched architecture that allows interworking of multiple RANs (3GPP and non-3GPP defined RANs) and provides high data rates and low latencies in comparison to previous 3GPP core networks (e.g. UMTS).

The EPC has various functional entities, as indicated by figure 2.1, working together to provide mobility, security, charging and Quality of Service (QoS) support. The functional entities relevant to this research are those entities providing the PMIPv6 mobility management functionality and include the Packet Data Network Gateway (PDN-GW), Serving Gateway (S-GW) and the evolved Packet Data Gateway (ePDG). The PDN-GW provides access to external Packet Data Networks (PDNs) like the Internet, and has functionality that includes: IP packet routing and forwarding, IP address allocation and is the mobility anchor during inter-system mobility between 3GPP and non-3GPP RANs. The S-

GW is the access gateway for LTE and the entry point towards the EPC, and has functionalities that include: IP packet routing and forwarding, packet buffering when the UE is in idle mode and is the mobility anchor for intra-3GPP mobility [2] i.e. mobility between 3GPP defined access networks. The ePDG [4] provides access to the EPC from non-3GPP RANs (e.g. WLAN) and has functionalities that includes: encapsulation/de-capsulation of packets for IPSec [27] (security association between the UE and the ePDG), enforcing QoS policies and IP packet routing and forwarding [4]. Matters concerning the rest of the functional entities of the EPC can be found in the technical specifications [2] [4]; a brief overview is also given in Appendix A.1 of this dissertation. 3GPP defines various logical reference points between the EPC entities [10]. The reference points relevant to this research are the S5 and S2b/S2a reference points; they provide user plane tunnelling management and PMIPv6 mobility support. The S5 reference point is defined between the S-GW and PDN-GW, and the S2a/S2b reference points are defined between the non-3GPP access gateways (i.e. ePDG) and the PDN-GW. The reference points are shown in figure 2.1.

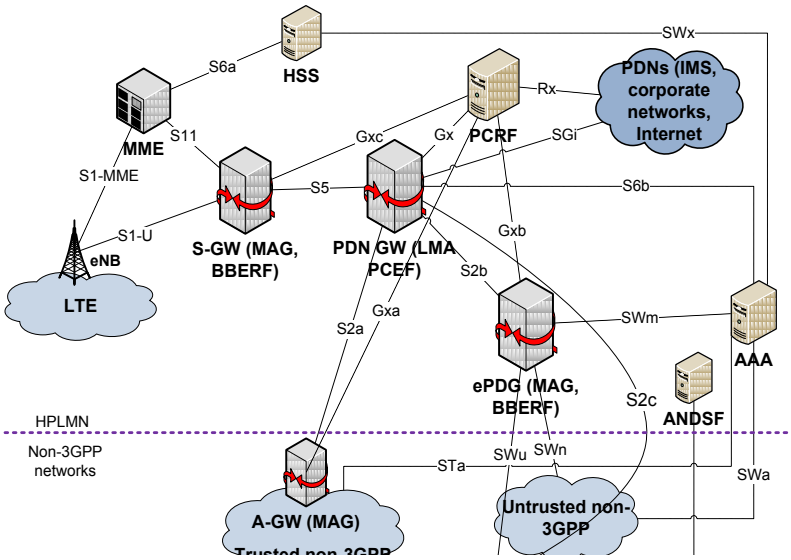

Figure 2.1: 3GPPs Evolved Packet Core architecture [4]

2.1.2 Mobility management in the Evolved Packet Core

The 3GPP standardisation body aimed at providing not only a common core network for heterogeneous RANs but also mobility between these RANs. Mobility refers to the movement of UEs (changing their point of attachment) from one RAN to another in the EPC.

Mobility management is required for ensuring that the end-user‟s ongoing sessions is maintained as they change their point of attachment to the EPC.

Providing session continuity support in IP networks has been researched extensively since as the UE changes its point of attachment to the network the IP address of the UE changes. Without a mobility management solution this IP address change results in the discontinuity of any ongoing sessions of the UE, since the sessions are tied to a specific IP address and can usually not survive an IP address change. To this end many mobility management solutions exist in the literature and for the EPC, 3GPP standardised the use of network- and host-based mobility management solutions [18], [17]. For intra-3GPP mobility (i.e. mobility between 3GPP access network only) the GPRS Tunnelling Protocol (GTP) [28] or PMIPv6 mobility approach can be used for providing session continuity, and for mobility between 3GPP and non-3GPP access networks the PMIPv6 or DSMIPv6 mobility protocols can be used.

The sub-sections that follow discuss the mobility approach for 3GPP to non-3GPP access networks since this mobility scenario has greater relevance to this research.

2.1.2.1 Host-based mobility management with DSMIPv6

Session continuity with DSMIPv6 is achieved by allowing the UE to be always reachable using the same IP address, called the Home Address (HoA) [29]. The HoA is assigned to the UE from its home network i.e. where the IP address is topologically correct, and in EPC the UE is always considered to be in its home network when it is attached to a 3GPP access network (which in terms of DSMIPv6 is known as home link). Whenever the UE moves between the 3GPP accesses, the UE will always use the same HoA.

When the UE moves outside of its home network i.e. to a foreign network, the HoA is no longer topologically correct for routing purposes and results in the UE configuring a local IP address, called the Care-of Address (CoA) [29]. With the EPC the UE is attached to a foreign network when using non-3GPP access networks (e.g. WLAN). To maintain any ongoing session the UE updates its current point of attachment (i.e. the CoA) by sending a Binding Update (BU) mobility signaling message containing its HoA and CoA to an entity situated in its home network, called a Home Agent (HA) [29]. When the HA receives the BU message creates an association between the UE‟s HoA and CoA, called a binding, and stores the binding in a conceptual data structure called a Binding Cache (BC). Once the binding has been established at the HA, it replies with a Binding Acknowledge (BA) mobility signaling

message and establish its end-point of a tunnel towards the UE. The UE, upon receiving the BA message, establishes its end-point of the tunnel and also maintain a binding in a conceptual data structure called a Binding Update List (BUL). After this procedure a bi-directional tunnel exists between the UE and HA through which the UE‟s data will be tunnelled. Hence, for downlink packets arriving at the HA and addressed to the HoA of the UE, the HA will intercept, encapsulate and forward the packets in the tunnel to the UE‟s current point of attachment (i.e. CoA). Normal processing of the tunnel header at the UE will result in the de-capsulation and processing of the packets. The HA functionality is located in the PDN-GW and the S2c reference point is used for the BU/BA messages, refer to figure 2.1. A typical Binding Cache Entry (BCE) and Binding Update List Entry (BULE) consist of the HoA, CoA and a lifetime associated to the binding. The lifetime indicates how long the binding should be kept active in the HA, before it is deleted. A BCE and BULE are managed using the HoA as look-up key.

Note: Session continuity in the UE is ensured by configuring the CoA on the physical network interface and configuring the HoA on a logical interface (also known as a virtual interface). This is because; when the UE de-capsulate the packets the destination IP address of the packets will be the HoA while the IP address on the physical interface is the CoA. Configuring the HoA on the logical interface makes the applications running on the UE oblivious to the changing CoA during UE movements. Thus, since the applications only see the HoA on the logical interface, session continuity is maintained. In addition to the logical interface in the UE, the UE also requires a MIP stack in its protocol stack. The Mobile IP (MIP) stack provides the necessary software logic that enables the UE to process and orchestrate the mobility signalling (i.e. the BU and BA messages) with the HA.

2.1.2.2 Network-based mobility management with PMIPv6

PMIPv6 provides network-based mobility support in the EPC and unlike DSMIPv6, mobility is provided without requiring the UE to be involved in any mobility related signaling and does not require the UE to implement a MIP stack [19], [18]. The mobility functionality of the UE is instead relocated to a functional entity within the network called a Mobile Access Gateway (MAG) [19] [18]. The MAG is responsible for detecting the UE‟s movements and for registering the current location of the UE by sending and receiving mobility signalling (Proxy Binding Update (PBU) and Proxy Binding Acknowledge (PBA) messages) on behalf of the UE to another functional entity called the Local Mobility Anchor (LMA) [19] [18].

The current location of the UE is indicated with a Proxy Care-of Address (P-CoA), which is the IP address of the egress interface of the MAG towards the LMA. The LMA can be considered as an enhanced HA and is responsible for maintaining the reachability of an UE connected to the EPC. The LMA is also in charge of allocating unique IPv6 Home Network Prefixes (HNPs) to the UE and is also the topological anchor point for the UE‟s HNPs. The UE uses the HNP to configure an IPv6 HoA using a procedure called stateless address auto-configuration, whereby the HoA is constructed by concatenating the HNP with the unique interface identifier of the physical network interface the UE is utilising to attach to the network.

Similar to DSMIPv6, the UE‟s traffic will be sent on a bi-directional tunnel, but with the tunnel end-points being the LMA and MAG. When the UE changes its point of attachment from its current MAG to a new MAG (nMAG), the LMA will update the location (with the new P-CoA) of the UE in its BC, assign the same HNP to the UE at the new point of attachment and establishes the bi-directional tunnel to the nMAG. Assigning the same HNP to the UE will ensure that the UE always configure the same HoA and thus ensuring session continuity during UE mobility. For downlink packets arriving at the LMA matching the HNP of the UE, the LMA will encapsulate and forward the packets on the tunnel towards the MAG [18]. The MAG, after receiving the packets, will de-capsulate and forward the packets to the UE on the access network [19]. The LMA functionality is located in the PDN-GW and the MAG functionality is located in the access gateways e.g. S-GW and ePDG, as shown in figure 2.1. The bi-directional tunnel and PBU/PBA messages are used on the S5, S2a and S2b reference points of the EPC. Unlike DSMIPv6 where there is a distinction between home network and foreign network, in PMIPv6 the UE is assumed to always be in its home network irrespective of whether it is attached to a 3GPP or non-3GPP access network.

The BCE maintained by the LMA is more advanced than that of the HA in that it contains additional entries: an UE identifier (UE-ID) which is a unique International Mobile Subscriber Identity (IMSI), the UE‟s HNP, the Access Technology Type (ATT) indicating the type of access network (i.e. LTE, WiFi, etc.) the UE is using to attach to the EPC, the current location of the UE which is the P-CoA and the Access Point Name (APN) identifying the PDN the UE is connecting to/receiving services from [19]. The BCE‟s are looked up on a per (UE-ID, APN) [19] tuple basis. The MAG maintains a BUL with similar entries to the BC.

2.2 IP flow mobility in the Evolved Packet Core

The granularity of access network connectivity and inter-system mobility based on [4] is per PDN connection (A PDN Connection is the association between a UE represented by an IPv6 HNP and a PDN [19] and is the name given to the IP connection (or mobility session) the UE has established to a PDN), meaning that when a handover occurs the UE‟s entire PDN connection is moved from the source to the target access network. IP flow mobility provides a finer granularity for access network connectivity and inter-system mobility [8] [26] by allowing the possibility of applying the mobility procedures to individual IP flows within a PDN connection (an IP flow is defined as in chapter 1). This implies that instead of moving the entire PDN connection (with all its IP flows) to a new access network, only a subset of the IP flows are moved to a new access network while the rest of the IP flows are kept on the source access network simultaneously.

In release 10 [8] 3GPP standardised an IP flow mobility solution for allowing an UE to simultaneously connect to a 3GPP access and a WLAN access and exchange different IP flows belonging to the same PDN connection through these accesses. The solution also allows the MNOs to indicate how the IP flows are routed through the available access systems and to selectively offload some traffic (e.g. best effort traffic) to WLAN while using LTE for the other traffic (e.g. traffic with specific QoS requirements) [8]. This is usually referred to as WLAN offload. The IP flow mobility solution is based on DSMIPv6, but due to the strong interest from MNOs for a network-based IP flow mobility solution using PMIPv6, 3GPP has started a study item [30] to develop a PMIPv6-based IP flow mobility solution. From a recently produced technical report [26] on network-based IP flow mobility in the EPC, 3GPP is considering to use the concepts of the DSMIPv6-based IP flow mobility solution and apply it to the PMIPv6 protocol for IP flow mobility. However, these concepts cannot be applied to the PMIPv6 protocol since there are some issues (that will be addressed in this research, and will be discussed within this section) with the protocol in supporting these mechanisms that is not addressed by the 3GPP. Thus, in this section a review is given on the DSMIPv6-based IP flow mobility solution of 3GPP to highlight the technical mechanisms of the solution. This will enable the identification and evaluation on the missing functionality in PMIPv6 to apply the mechanisms of the DSMIPv6 IP flow mobility solution.

2.2.1 3GPP's standardised DSMIPv6-based IP flow mobility solution for the EPC

The DSMIPv6-based IP flow mobility solution consists of the following concepts adapted from the IETF standardisation body for the DSMIPv6 protocol:

- A mechanism, called Multiple CoA Registration [31], for allowing the UE to connect with multiple interfaces to the EPC and registering the multiple CoAs of the interfaces to a single HoA for session continuity.
- A mechanism, called Flow Bindings [32], for enabling flow-based routing in the HA and UE and allowing the UE to set forwarding preferences for the IP flows at the HA.

2.2.1.1 Multiple Care-of Address registrations for session continuity in IP flow mobility

IP flow mobility explicitly requests for the UE to connect to the EPC using multiple interfaces (i.e. LTE and WLAN) such that some IP flows can be routed through the one interface (i.e. WLAN) while the rest remain on the other interface (i.e. LTE). When a UE with multiple interfaces uses DSMIPv6 in the EPC for mobility management, it cannot use multiple interfaces to send and receive data while taking advantage of session continuity provided by the DSMIPv6 protocol [31]. This is because the DSMIPv6 protocol supports only session continuity for single-interfaced UEs meaning that the HoA assigned to the UE can only be associated with one CoA at a time. The mechanism adopted from [31] allows an UE to register multiple CoAs to a single HoA (i.e. multiple bindings) for the purposes of ensuring session continuity during interface handoffs. To register multiple bindings at the PDN-GW/HA, the UE is enhanced to generate a Binding Identification (BID) [31] number for each of the CoAs it intends to register to a HoA, and the HA functionality is enhanced to process BID information received from the UE. For example, if the UE has HoA1 and configures two CoAs (CoA1 and CoA2), the UE would generate a BID for each HoA-CoA binding it intends to register i.e. HoA1-CoA1 has a BID of 1 and HoA1-CoA2 has a BID of 2. The BID, along with the HoA and CoA, is sent in a BU message (the technical extensions to the BU messages are discussed in [31]) to the PDNGW/HA. When the PDNGW/HA receives a BU message with a BID, it creates a separate BCE for each unique BID it receives from the UE.

Based on the enhancements for multiple CoA registrations, a typical BC in the PDNGW/HA when the UE is not on its home network is shown in figure 2.2. When the UE is

connected with one interface to its home link (e.g., LTE) and one interface to a foreign link (e.g. WLAN) the CoA field for the home link according to this extension will be set to the HoA. Hence, a BC in the PDNGW/HA incorporating this scenario is shown in figure 2.3.

Home Address	Care-of address	Binding ID
HoA1	CoA1	1
HoA1	CoA2	2

Figure 2.2: Binding Cache in PDNGW/HA supporting multiple CoAs registration (foreign network case)

Home Address	Care-of address	Binding ID
HoA1	HoA1	1
HoA1	CoA2	2

Figure 2.3: Binding Cache in PDNGW/HA supporting multiple CoAs registration (home and foreign network case)

The PDNGW/HA uses the BID information as a look-up key to identify individual bindings of the UE when processing BU messages. Each BID is unique for a given HoA, which means that different UEs can use the same BID value [8].

2.2.1.2 DSMIPv6 enhancements for flow-based routing and management

In order to route packets at an IP flow level and through any access, the DSMIPv6 protocol is enhanced to allow the UE to bind one or more IP flows to a particular CoA without affecting other IP flows using the same HoA.

The UE is enhanced to request to create flow bindings at the HA [8], where a flow binding is an association between a routing filter and a BID. A routing filter is a set of IP header parameter values/ranges used by the HA to identify a packet of an IP flow, examples of which include: the source and destination IP addresses, source and destination port numbers and transport protocol used (e.g. TCP or UDP). The BID is used to refer to a particular routing address (i.e. CoA) for the IP flows. Each flow binding has a unique Flow Identification (FID) number. The FID is a number generated by the UE when an IP flow is established and is used for identifying and referring to the flow bindings of the UE. The flow bindings are stored in an enhanced BC and BUL data structure of the HA and UE respectively, and sent in BU message. The HA acknowledge the receipt of the flow bindings with BA message. The necessary extensions to the BU and BA messages are detailed in [32].

When the flow bindings has been created at the HA and downlink packets arrive at the HA for the UE, the HA will match the packets to all the routing filters installed by the UE,

and forward the matched packets to CoA associated to the routing filter. These packet processing rules are different to how the HA normal process packets, since under normal circumstances when the HA intercepts packets addressed to the HoA of the UE, it would forward the packets to the corresponding CoA in the BC. Figure 2.4 shows an example of a BC supporting the multiple CoA registration and flow-based routing enhancements for IP flow mobility in the PDNGW/HA. From figure 2.4, all TCP IP flows and IP flows with source address equalling IPy will be forwarded to CoA1. Similarly, any UDP traffic will be forwarded to CoA2.

To modify the forwarding path of any IP flow in the HA, the UE needs only update the FID-BID association of the flow binding. Figure 2.5 shows a modified routing path for the TCP IP flows of figure 2.4. Now, according to figure 2.5, all TCP IP flows will be forwarded to CoA2.

Home Address	Care-of Address (Routing Address)	Binding ID	Flow ID	Routing filter
HoA1	CoA1	1	1	*,*,*,*,TCP
			2	Src_addr = Ipy,*,*,*,*
HoA1	CoA2	2	3	*,*,*,*,UDP

Figure 2.4: PDNGW/HA supporting flow based routing

Home Address	Care-of Address (Routing Address)	Binding ID	Flow ID	Routing filter
HoA1	CoA1	1	1	*,*,*,*,TCP
			2	Src_addr = Ipy,*,*,*,*
HoA1	CoA2	2	3	*,*,*,*,UDP
			1	*,*,*,*,TCP

IP flow handover to CoA2

Figure 2.5: PDNGW/HA supporting flow based routing (flow handover)

2.2.2 Issues with PMIPv6 for supporting IP flow mobility in the EPC

As previously mentioned, 3GPP proposed that the mechanisms of the DSMIPv6-based IP flow mobility solution should be applied to the PMIPv6 protocol for enabling IP flow mobility. However, 3GPP did not specify exactly how the mechanisms are to be applied and instead assumed that since the protocols are similar, the mechanisms can be applied. This is not the case when looking at the working principles of the PMIPv6 protocol. Firstly, in the case of the multiple CoA registration mechanism, the BID is an identification number used to distinguish multiple bindings registered by the UE and each BID is generated and managed by the UE. In PMIPv6 the mobility of a multi-interfaced UE is managed in different independent MAGs and the UE is completely unaware of the existence of these MAGs or the P-CoAs. The UE is also not involved in managing its mobility with the LMA. Therefore, the

BID loses its meaning with PMIPv6 since the creation and management of BIDs depends on the UE knowing the CoA and being involved in sending this information to the network. Secondly, since the flow-binding management of the flow-based routing mechanism is based on the UE generating and associating a FID to a BID and since the BID is not applicable to the PMIPv6 protocol, the flow-binding management of the flow-based routing mechanism is also not applicable to the PMIPv6 protocol.

Additionally, as discussed in sub-section 1.1.2.2, session continuity with PMIPv6 is achieved by allocating the same HNP to the UE as it changes its point of attachment within the network, this way the UE configures the same HoA and the ongoing session will not require reestablishment due to interruption. This type of handover scenario assumes the UE is using the same network interface at the new point of attachment, since to configure the same HoA not only must the HNP be the same, but the interface identifier must also be the same. The interface identifier is a derivative of the Medium Access Control (MAC) address of the interface and is the last 64-bits of an IPv6 address that is unique to the 64-bit HNP (The UE appends its interface identifier to the received HNP when constructing an IPv6 HoA). The same session continuity methodology cannot be applied when the UE has multiple interfaces attached to the PMIPv6 domain for simultaneous use (as is the assumption for IP flow mobility). In this scenario the LMA assigns a unique HNP for each of the attached interfaces of the UE (with each interface having its own BCE) and when a handover is performed the LMA will assign the HNP of the Previous Interface (PIF) to the New Interface (NIF), update the BCE of the NIF with the new HNP and remove the BCE of the PI. In this instance the LMA assumes that by assigning the same HNP enables session continuity between the two interfaces, but several issues exist with this logic:

1. Assigning the same HNP to the NIF of the UE does not mean that the same IP address will be configured. In fact, a completely different IP address (even if the HNPs are the same) is configured on the NIF because each physical interface has a unique interface identifier. This means that for the services that has been moved to the NIF will be discontinued as the destination IP address of the packets will be different from the IP address on the NIF.
2. Deleting the BCE of the PIF means that the services using the PIF will be discontinued.
3. Updating the NIF with new HNP means that the previous HNP will be replaced, which also means that the services using the IP address of the NI before the handoff will be discontinued (due to the NIF having to reconfigure a new IP address from the

received HNP) and will have to be re-established with the new IP address (from the HNP).

From the issues identified above it is clear that session continuity is not provided in an efficient way for handoffs with multi-homed UEs (meaning that the UE has multiple interfaces attached to the network and is sending and receiving data on these interfaces simultaneously). In IP flow mobility the UE is both multi-homed and IP flows are moved between 3GPP and non-3GPP accesses. Hence, unlike DSMIPv6 where the UE has a single HoA to which multiple CoA on the physical interfaces are bound and where this single HoA is always used e.g. on the destination IP address of the downlink IP packets of the UE, in PMIPv6 the destination IP addresses of downlink packets is the HoA configured on the physical interfaces.

Figures 2.6 and 2.7 illustrate the difference between the session continuity logic of DSMIPv6 and PMIPv6 for the IP flow mobility scenario. In figure 2.6a the UE has two IP flows; each addressed to the HoA, but tunnelled to different CoAs (CoA1 and CoA2) of the interfaces. When an IP flow is moved (figure 2.6b) the CoA changes (from CoA1 to CoA2) but the same HoA is kept, which means the IP flow will not be discontinued. In figure 2.7a shows a UE with two IP flows, each addressed to the HoA configured on the interfaces. When an IP flow is moved (figure 2.7b) the IP flow is discontinued (new HoA that is different than what the IP flow is bound to) at the new interface along with any other IP flows already existing on the new interface. Hence, comparing figure 2.6b and figure 2.7b, session continuity is maintained in the DSMIPv6 case (figure 2.6b) but not in the PMIPv6 case (figure 2.7b), since as can be seen in figure 2.7b, the HNPs of the new interface changes (from HNP2 to HNP1) and the HoA changes (from HoA2 to HoA3). The IP flows tied to HNP2 will be disconnected and the IP flows tied to HNP1.

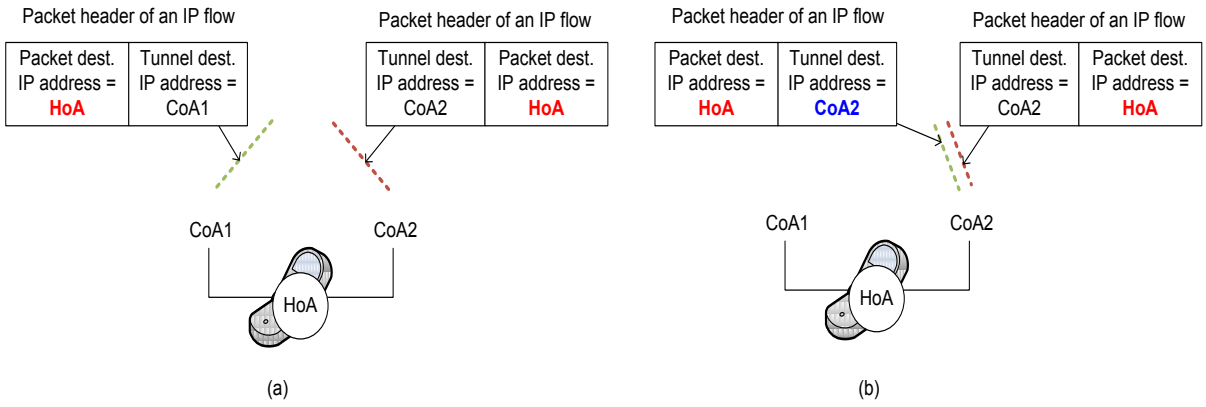

Figure 2.6: IP flow handover in DSMIPv6 where (a) is before the handover, and (b) after the handover

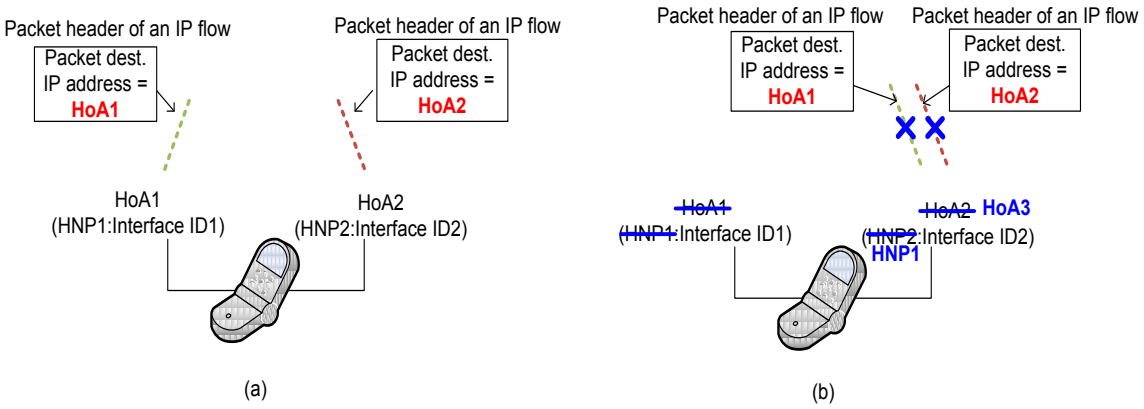

Figure 2.7: IP flow handover in PMIPv6 where (a) is before the handover, and (b) after the handover

Hence, for an IP flow mobility solution for PMIPv6 there needs to be a mechanism to provide session continuity and a mechanism for flow-based routing and management. These mechanisms are not provided by the 3GPP standardisation body.

2.3 Related work

In this section a review is given on work related to IP flow mobility with the PMIPv6 protocol. The objective of this review is to identify how these proposed IP flow mobility solutions address the issues outlined in 2.2.2 when considering session continuity for IP flow handoff, and how flow-based routing and management is enabled with PMIPv6

2.3.1 The IETF standardisation body efforts towards PMIPv6-based IP flow mobility

The IETF standardisation body (responsible for defining PMIPv6) is also working towards defining a PMIPv6-based IP flow mobility solution, and since the EPC incorporates many other IETF defined protocols (e.g. Diameter [33](used by the AAA and HSS in the EPC), IKEv2 [**34**] (used the ePDG to establish the security association with the UE), etc.), the IETF activities in the area of IP flow mobility support with PMIPv6 is relevant to this research. As 3GPP‟s proposed solution for DSMIPv6-based IP flow mobility are based on mechanisms defined by the IETF, the IETF proposed IP flow mobility mechanisms for the PMIPv6 protocol could be adapted and applied to the EPC. Much of the extensions proposed to the PMIPv6 protocol by the IETF are published in the form of Internet drafts. Internet drafts are temporary documents that expire after 6 months after they have been issued and once it has matured sufficiently are published as IETF Request for Comments (RFCs) i.e. standards.

After the expiration of an Internet draft, the work addressed in the draft is considered obsolete. Therefore, in reviewing this work it is recommended that the latest version of any cited Internet draft be examined as of June 2013. The Internet draft, *Proxy Mobile IPv6 Extensions to Support Flow Mobility* [35] , represents the most recent output from the IETF standardisation body, and from this draft it is apparent that they too are adopting the mechanisms of the DSMIPv6 protocol for enabling IP flow mobility with PMIPv6, and unlike the 3GPP standardisation body, the IETF proposes how these mechanisms can be applied to PMIPv6 and also proposes enhancements to PMIPv6 for ensuring session continuity for the mobility scenario of IP flow mobility. The proposed solutions are discussed in the following section.

2.3.1.1 Session continuity enhancements to PMIPv6 for IP flow mobility

The IETF, starting off with an evaluation of the multiple interface support procedure of the LMA, identified that the HNP allocation and BCE management procedures of the LMA needs to be enhanced, since with the standardised procedures session continuity cannot be maintained. The evaluation also revealed that enhancements to the UE are inevitable for supporting session continuity. Thus, in addition to the protocol enhancements IETF also proposes enhancements for the UE.

2.3.1.1.1 Protocol enhancements

IETF proposes three types of HNP allocation procedures that the LMA can support for enabling session continuity during IP flow mobility:

1. The LMA allocates the same unique HNP to each of interfaces the UE is attaching to the network. This is not the default behaviour of the LMA since the same HNP is not just allocated for handover, but also for simultaneous attach. IETF proposes enhancements to the PBU/PBA messages for allowing the MAG to indicate to the LMA that the same HNP should be assigned, and they propose enhancement to the PBU processing logic of LMA in order for the LMA to deduce that the same HNP should be allocated to the UE when receiving such a request in a PBU message. The IETF claims that using this scenario in an IP flow mobility solution would reduce the amount of signaling in the network, since all the MAGs the UE is attached to will already have all the routing information (i.e. HNP) in advance to forward the UE‟s IP flows, thus the LMA (who is the decision entity for initiating IP flow mobility) can simply move an IP flow between the MAGs of the UE.

2. The LMA follows the default HNP allocation procedure and assigns a new unique HNP to the UE for every interface. IETF proposes additional signaling messages between the LMA and MAG to indicate the previously assigned HNP of the UE to the new MAGs, hence enabling the new MAGs to be aware of the HNPs for which the UE is going to receive IP flows on. Two new signaling messages are defined for this scenario: a Flow Mobility Initiate (FMI) and Flow Mobility Acknowledge (FMA) message [35]. The FMI message is sent from the LMA to the MAG and the FMA message is sent from the MAG to the LMA in response to the FMI message, and indicates to the LMA whether forwarding of the IP flow can commence or not. The FMI and FMA messages are sent independently of the PBU/PBA messages and also indicate any IP flow information (i.e. FID, BID, etc) to the new MAG (if the MAG requires such information).

3. The LMA allocate a new HNP as well as the HNPs in use by the other interfaces of the UE. This scenario is a hybrid of (1) and (2) and presents no additional signaling messages, since IETF proposes that the additional HNPs of the UE should be sent in the PBA messages during the initial attachment procedure of the UE interfaces.

In the second and third HNP allocation proposals it is noted that IETF only proposed signaling procedures for enabling these proposals, but not the actual enhancements to the LMA and MAG to incorporate the signaling procedures in their default behavioral logic, instead the enhancements are left for operator defined deployments. In addition, IETF also did not define how the LMA should manage its BC, since as mentioned previously; when moving an IP flow to a NIF while the PIF is still active, the previous BCE and HNP of the PIF will be removed and causing the IP flows on the PIF to be discontinued.

2.3.1.1.2 UE enhancements

At the UE the HoAs configured on the physical network interfaces are logically different even when using the same HNP for HoA configuration which means that even if session continuity can be achieved at the network side, the IP flows will be discontinued at the UE. The IETF proposed that the UE be enhanced with either the weak-host model [36] or the Logical Interface (LIF) [37]. The weak-host model is a mechanism enabling an UE to send/receive packets on any of its interfaces, even if the destination/source IP address of the packet do not match the IP address on the sending/receiving physical interface [36]. The mechanism for enabling the weak-host model comes standard in most UE operating systems and is a software configuration option for UE manufacturers when implementing the UE‟s IP stack. For example, Microsoft operating systems (Windows XP, Vista and Windows 7) and

Linux operating systems both support the weak-host model. The IPv4 and IPv6 implementation of Microsoft and Linux uses the weak-host model [38] and is even implemented in new generation mobile phone operating systems e.g. Android operating system. The Android operating system is based on a Linux kernel, and in many cases behaves like a Linux device [39]. For incoming packets, Android implements the weak-host model for both IPv4 and IPv6 [39].

The LIF allows the UE to provide a single interface view to the layers above IP (thus not changing the IP layer itself) [37], meaning that from the perspective of the IP stack and the applications (to which the application sockets will be bound), the UE has only one interface. When an IP address is configured on the LIF (i.e. a globally unique routable IP address from one of the HNPs of the physical interfaces), the applications on the UE will only use this IP address as source address. When a handoff occurs between the physical interfaces on the UE, the IP address change (i.e. HoA changes) on the physical interfaces is not visible to the applications. The physical interfaces on the UE are thus "hidden" from the IP stack and from the network nodes on the attached access networks [37]. Enabling the LIF in a UE requires the addition of a software component to the operating system of the UE. The specific details of the LIF in terms of operation and interface management are elaborated in [37]. This LIF is similar to the LIF mentioned in section 2.1.2.1 for DSMIPv6 UE.

2.3.1.2 Enhancements for flow-based routing and management

For flow-based routing management, the BC of the LMA is enhanced for allowing multiple P-CoA registrations and to associate each of the registrations with a BID. The BID is used for allowing the LMA to distinguish between the BCEs of the UE when using the proposed prefix allocation mechanisms of the previous section. With the scenarios of the previous section, the LMA can bind a HNP to multiple P-CoAs (which is also a similar concept to binding multiple CoAs to a single HoA as in [31]). In comparison to [31] where the BID is generated and managed by the UE, in this proposal the BID is generated locally by the LMA and the UE is not aware of the BIDs. The number of BCEs for the UE corresponds to the number of interfaces the UE is attaching to the network. The LMA is also enhanced with a Flow Binding Cache (FBC) [35], as shown in figure 2.8. The FBC is a conceptual list of Flow Binding Entries (FBE) and is maintained separately from the BC structure. Each FBE contains a FID, a Packet filter, a BID and FID priority (FID-PRI), and points to a specific BCE using the BID. IP flows can then be moved by simply updating the pointer of the FBE

with the BID of the interface to which the IP flow should be moved [35]; this is illustrated in figure 2.9 (i.e., the IP flow with a FID of 3 is moved to the 3GPP access). IETF re-uses the packet processing extensions of the HA (defined in [32]) for the LMA, meaning that for downlink packets arriving at the LMA and addressed to the HNP for the UE, the LMA will match the packets to the list of packet filters in the FBC of the UE and forward the packets to the P-CoA of the BCE to which the BID (of the FBC) points to.

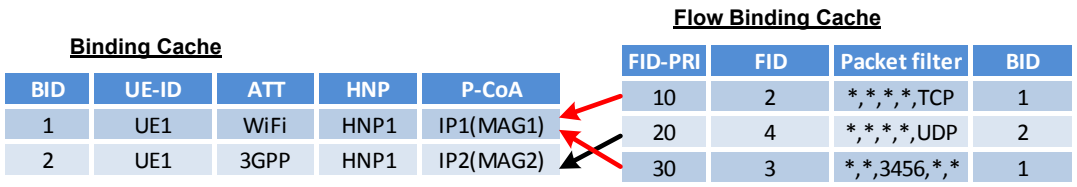

Figure 2.8: Binding Cache and Flow Binding Cache in a LMA enhanced with multiple P-CoA registrations, shared HNP and flow-based routing

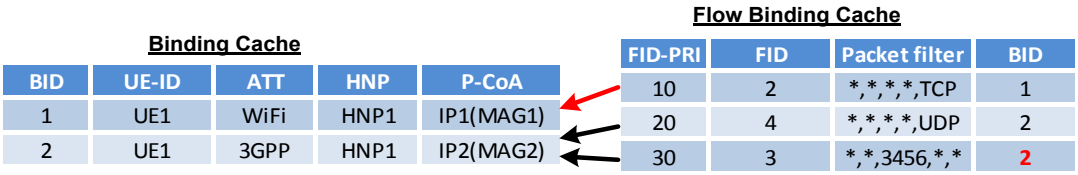

Figure 2.9: IP flow handover from WiFi to 3GPP access network

2.3.2 IP flow mobility solutions proposed in the literature

Even with the proposed PMIPv6 IP flow mobility solutions by the standardisation bodies, no standard has been recommended. Additional solutions exist in the literature that addresses IP flow mobility with the PMIPv6 protocol. The solutions are mainly based on the IETF defined PMIPv6 protocol and architecture. In this sub-section the most relevant PMIPv6-based IP flow mobility solutions proposed in the literature are reviewed and the merits and demerits discussed.

Trung *et al* [20] propose an IP flow mobility solution based on the IETF defined PMIPv6 architecture. This solution also enhances the LMA for session continuity during IP flow mobility and they enhance the protocol to support flow-based routing. For session continuity the authors base their solution on the second HNP allocation proposal of the IETF, but point out that with the IETF proposed solution, sending the IP flow information (using FMI message) to the MAGs is redundant since the MAG might not implement the flow-binding table and that the signaling procedures proposed by IETF for assigning the same HNP to the

UE for session continuity is incomplete. Hence, the authors proposed two signaling approaches for assigning the previous HNPs of the UE to the MAGs: a proactive and reactive signalling approach. In the proactive signaling approach when the LMA assigns a HNP to the UE, it will immediately signal this HNP (together with any other HNP) to all the MAGs to which the UE attaches. In the reactive signaling approach the HNP is shared with another attachment only when an IP flow is moved to a MAG where the HNP associated to that IP flow is not valid. Thus, when the LMA decides to move an IP flow and realises that the HNP used by that flow is not valid at the destination MAG, it will signal the HNP to the MAG [20]. In both signaling approaches, to enable the LMA to update a MAG with HNPs from the other attachments of the UE, the authors introduced two new signaling messages: a Home Network Prefix Update Request (HUR) and a Home Network Prefix Update Acknowledge (HUA) message [20]. The HUR message is sent by the LMA to the MAG to request the MAG to update with a HNP and the HUA is sent by the MAG to the LMA to inform the LMA that it is ready to forward packets for the received HNP. The authors provide the extensions to the LMA and MAG for enabling them to exchange HUR/HUA messages. The authors also assume that the UE implement the logical interface to support the signaling procedure and session continuity. For flow-based routing and flow management, the authors adopt the IETF proposed solution, refer to section 2.3.1.2.

To show the feasibility of the proposed IP flow mobility solution, the authors developed the IP flow mobility solution for the proactive signaling approach on a network simulation tool, Network Simulator version 3(NS-3) [40]. The simulation network topology consists of a WLAN and a WiMax access network, a LMA, two MAGs each serving a separate access network, and a UE. The authors provide throughput plots showing the behaviour of two UDP based applications and showing that by moving one of the UDP traffic to an alternative interface the throughput increases for that IP flow. The results the authors presented are merely showing a benefit for having IP flow mobility in a network and not actually showing the feasibility of their proposed mechanisms. The authors did not provide a thorough evaluation to show the effects their solution might have on the network, e.g. by sending additional signaling (the HUR/HUA) can easily bring about signaling overhead in the network because these messages will be sent on a UE-basis. Additionally, the enhanced packet processing logic of the LMA can introduce an additional delay when an IP flow is moved to a new access network (i.e. contribute to handover latency) and can also affect the overall throughput of the network (this is not shown in their results). It is also found that even in this work the authors did not clearly state the enhancements to the LMA and MAG for

session continuity instead only signaling is defined.

Choi *et al* [9] [41] propose a PMIPv6-based IP flow mobility solution that is also based on the IETF defined PMIPv6 architecture and is similar to the IETF proposed IP flow mobility solution, but the authors point out that the IETF proposal does not support the scenario where the UE wishes to initiate IP flow mobility; instead the solution only support the scenario where IP flow mobility is initiated by the network (i.e. LMA). UE-initiated IP flow mobility can be as a result of the end-user wanting a cheaper access network (e.g. WLAN) for their services. The authors define new UE-based IP flow mobility signaling procedures in which IP flow mobility is initiated either due to the UE connecting a new interface to the PMIPv6 domain or due to the UE explicitly requesting the LMA to redirect a particular IP flow from one interface to another. The latter procedure contains new signalling messages (Flow Mobility Indicate (FMI) [41] and Flow Mobility Acknowledge (FMA) [41]) that are sent from the UE to the MAG in order to initiate IP flow mobility and to send IP flow routing information. For ensuring session continuity in each of the use case scenarios the authors proposed that the LMA assign the same HNP to the interfaces of the UE (this is similar to scenario 1 of the IETF proposed solution) and design their signaling procedures around this concept. The authors also assume that the UE has a LIF to complement session continuity in their proposed signaling procedures. For flow-based routing and management the authors introduce two components: a flow interface manager, interfacing with the LIF in the UE, and a flow binding manager in the LMA. These components are used for selecting the access network through which IP flows should be routed and is used for managing the flow bindings of the UE and LMA. The authors reuse the flow binding concept of [32] but redefine the meaning of a flow binding. In the LMA a flow binding is the association between a routing filter and a priority list of Access Technology Types (ATTs), and in the UE a flow binding is the association between a routing filter and a priority list of interfaces. This is different from the base concept [32] in that a flow binding is defined as the association between the routing filter and BID. Each component maintains a list of flow binding entries (refer to figure 2.10 and 2.11) containing a FID, a priority, a routing filter, a priority list of ATTs/interfaces, a Type and a Lifetime field. The FID and routing filter are the same as in [32] and the priority field indicates the filtering order of the entries in the list. The Type parameter indicates whether the flow binding is static or dynamic. A Type field set to static indicates that the flow binding cannot be changed and are either pre-configured by the network operator (if the flow binding is in the flow binding list in the LMA) or the end-user

(if the flow binding is in the flow binding interface list in the UE). In contrast, when the flow binding has a Type set to dynamic, the flow binding can be changed during its validity period (which is indicated by the lifetime field) and can be changed by either the network or the UE. The packet processing procedures of both the LMA and UE is enhanced such that when downlink packets arrive at the LMA, the packets are matched against the packet filters in the flow binding list, and when a match is found the LMA selects the highest priority access network corresponding to the matched packet filter and forward the packets on the corresponding tunnel to the MAG. For uplink packets originating from the UE a similar process occurs as in the LMA, but the highest priority interface is selected for forwarding the packets on.

ID	Priority	Routing filter	ATT Priority List	Type	Lifetime
1	4	<3ffe:34ab::11f,*,80,*TCP>	MAG#1 (3G) -> MAG#2 (WLAN)	Dynamic	180sec
2	3	<*,*,3768,*,UDP>	MAG#2 (WLAN) -> MAG#1 (3G)	Static	∞

Figure 2.10: Flow binding list in the Flow Binding Manager in the LMA

ID	Priority	Routing filter	Interface Priority List	Type	Lifetime
1	4	<3ffe:34ab::11f,*,80,*TCP>	Interface#1 -> Interface#2	Dynamic	180sec
2	3	<*,*,3768,*,UDP>	Interface#2 -> Interface#1	Static	∞

Figure 2.11: Flow binding interface list of the Flow Binding Interface Manager in the UE

To show the feasibility of the proposed IP flow mobility solution the authors performed proof of concept testing in the NS-3 simulation environment. The simulation network topology consists of three access networks (WLAN, WiMax and 3G) and a LMA managing three MAGs corresponding to the access networks. The proof of concept results shows that each of the UE-initiated IP flow mobility procedures can be achieved with their solution. However, the authors did not evaluate the performance of their proposed solution to show the effects it has on the network or end-user experience. For example, the flow binding manager can lead to scalability issues since any UE can create a flow binding entry which can easily result in the list expanding to thousands of entries, and since the LMA would have to match all incoming packets to the routing filters in the list, the LMA could end up being a bottleneck node in the network. This solution is also a generic solution.

2.4 Discussion

The 3GPP standardisation body has defined IP flow mobility as a means for enabling MNOs to offload traffic from the EPC network and so alleviating congestion and ensuring that the end-user‟s quality of experience is maintained. This chapter has presented the state of the art regarding 3GPP‟s IP flow mobility support with the PMIPv6 protocol in the EPC and have identified issues involving flow-based routing and that which impacts session continuity as being overlooked by the 3GPP. It has become evident that the IETF standardisation body has been a key enabler in achieving IP flow mobility in the EPC, and the fact that the 3GPP adopts most of the IETF standards wherever possible into the EPC and since the standardised DSMIPv6-based IP flow mobility solution are based on IETF defined standards, deems it necessary to consider the mechanisms proposed by the IETF for PMIPv6 IP flow mobility in the EPC. Hence, the state of the art according to what IETF has proposed for IP flow mobility with the general PMIPv6 architecture has also been discussed, and it was found that IETF has proposed mechanisms enabling flow-based routing as well as ensuring session continuity. In this research the IETF proposed mechanisms for IP flow mobility support with PMIPv6 is adopted to overcome the session continuity and flow-based routing issues associate with PMIPv6. In the next chapter the proposed IP flow mobility solution for the EPC architecture is presented. The proposed solutions in the related literature are variations of the IETF solution, but also present and highlight additional considerations that have been overlooked by the IETF, like considering the UE‟s decision to trigger and manage IP flow mobility. Having reviewed the related IP flow mobility solutions, it became apparent that the authors fail to provide a proper performance evaluation since no evaluation is given on the effects their solution could have on the MNOs network or the end-user quality of experience, nor is the solutions developed for 3GPPs EPC. The related works are also all implemented in a simulation environment, whereas in this research the proposed PMIPv6-based IP flow mobility solution will be evaluated and implemented in a real emulated EPC network environment.

Chapter 3

Proposed PMIPv6-based IP flow mobility functionality for the Evolved Packet Core

The previous chapter, in reviewing the standardised DSMIPv6 IP flow mobility solution of 3GPP and related literature, highlighted the necessary mechanisms for realising IP flow mobility i.e. flow-based routing, IP flow information management and ensuring session continuity during IP flow handoffs. The previous chapter also highlighted the following missing functionality of the PMIPv6 mobility functionality in the EPC in supporting these mechanisms for IP flow mobility: the standard PMIPv6 handoff procedures cannot ensure session continuity during handoffs between the UEs interfaces and due to the UE not being involved in the orchestration and processing of mobility signaling the flow-based routing and management mechanisms cannot be applied to PMIPv6 directly. The 3GPP standardisation body did not recommend solutions to overcome these issues, having assumed that due to the similarities of DSMIPv6 and PMIPv6, the mechanisms could be applied to PMIPv6. This chapter proposes enhancements to the PMIPv6 mobility functionality of the EPC architecture in order to support IP flow mobility. The enhancements are based on the proposals of the IETF standardisation body, since one of the policies of the 3GPP standardisation body is that of adopting IETF defined standards; this is evident from their standardised DSMIPv6 IP flow mobility solution as well.

The chapter begins by outlining the design requirements and considerations for supporting IP flow mobility with the PMIPv6 in 3GPPs EPC architecture; these requirements

and considerations were formulated from the review on the standard 3GPP DSMIPv6 IP flow mobility solution, the related works and the requirements set forth by the 3GPP standardisation body [30], [26]. The proposed PMIPv6-based IP flow mobility solution is then presented, with special emphasis on the session continuity and flow-based routing and IP flow management aspects. The functional extensions of the PMIPv6 components within the EPC are then discussed.

3.1 Functional Requirements

Based on discussions in the previous chapter, an IP flow mobility solution should introduce the following functional requirements.

3.1.1 Multiple simultaneous interface connectivity support (i.e. Multihoming)

The UE, when under the coverage of multiple access networks, should be able to communicate using multiple access network simultaneously if the UE is authorised by subscription to access all the PDNs and all the involved access networks [30], [26]. This is a fundamental requirement for enabling IP flow mobility, since the concept assumes that during IP flow handoff the UE maintains the connectivity with its previous interface (i.e., access network). Keeping the previous interface active ensures that the rest of the IP flows (on the previous interface) do not get disconnected. Without multihoming support in the network side and the UE, IP flow mobility would not be possible as in this case the only mobility scenario that would be possible in the network is where all the UEs IP flows are moved to a new interface, which is the same as the normal vertical handover scenario.

3.1.2 Ensuring session continuity during IP flow handoff

The IP flow mobility solution should provide session continuity during IP flow handoffs. As explained in the previous chapter, the goal of any mobility management solution is to maintain the UEs ongoing session as it moves. This goal should still hold for IP flow mobility as it is an enhancement of the EPC mobility functionality and since the UEs IP flows are being moved between its interfaces and between access networks.

3.1.3 Flow-based routing and IP flow information management

The most important goal of this research is to be able to move an IP flow from one access network to another with a view to enable smart WLAN offloading while augmenting the end-user quality of experience. To achieve this goal, the network has to able to route traffic on an IP flow level as well as allow the management of the IP flow information in order to specify the route a particular IP flow should take. At the end, it should thus be possible to select one access network when an IP flow is started and re-distribute the IP flows to or from an UE between the accesses while connected [30], [26].

3.2 Design Considerations

The EPS is characterised for providing enhanced network performance like low communication delay, high communication quality and higher user data rates equating to broadband performance [42]. Any enhancements to the EPC architecture should take into account considerations discussed below:

3.2.1 Negligible effect on the end-user Quality of Experience

The end-user Quality of Experience (QoE) binds together the user perception, experience, and expectations to application performance, typically expressed by Quality of Service (QoS) parameters [43]. Many factors influence the QoS of a given application like the service quality of the network, the associated hardware and software that make up the application, and the performance of the underlying transport network [44]. From the viewpoint of the application layer, the EPC architecture is the underlying transport network, and since this research revolves around the EPC architecture, consideration should be given to the effect IP flow mobility has on the EPC network performance, in particularly whether it introduces any overhead in the EPC entities. Overhead refers to the processing in the EPC entities that is directly attributable to the IP flow mobility solution itself. In this research, the packet and mobility signaling processing are of particular importance, since these procedures impact the end-to-end delay (excessive processing in a network node) and delay variation requirements of applications. The proposed IP flow mobility functionality, introduced in the next section of this chapter, introduces enhancements to the packet and mobility signaling processing procedures of the LMA functionality (refer to figure 2.1) in the PDN-GW.

From a mobility management perspective, a characteristic of the EPC is that it optimises

the mobility functionality by offering minimal signaling overhead and minimal handover interruption time [42], important metrics that indicate to MNOs whether deploying a particular facility in their network would bring about additional signaling delay or degrade the performance of their network nodes ultimately affecting the end-user QoE. An IP flow mobility solution that provides flow-based routing, management and ensuring session continuity during IP flow handoffs, but causes excessive signaling within the EPC network or that causes a significant latency when offloading an IP flow, are undesirable. It is thus important to consider these parameters when evaluating the performance of the IP flow mobility process, especially since bandwidth intensive video streaming services are the most likely service to be offloaded to WLAN access networks. Video streaming services are quickly becoming the most popular service amongst end-users and this type of service has to conform to certain application requirements in order to be of an acceptable quality to the end-user. The IP flow mobility enhancements proposed in this dissertation could affect these requirements for the video streaming service.

The proposed IP flow mobility solution should also dictate a minimal amount of alterations to the UE. A benefit of network-based mobility is that it does not require the UE to be involved in the orchestration and processing of mobility signaling messages, which means that mobility can be provided to UEs without affecting its battery power consumption (processing mobility messages causes strain on the UEs battery consumption). An IP flow mobility solution that causes excessive processing in the UE is thus impractical, since the UE is required to operate multiple interfaces simultaneously for IP flow mobility, which could affect its battery power consumption. Hence, procedures related to IP flow mobility and requiring advanced processing should be limited to the core network.

3.3 Proposed IP flow mobility scheme for the EPC

This section details the proposed PMIPv6-based IFOM solution for the EPC. The first sub-section gives an overview of the architecture, detailing the EPC components requiring enhancements for IP flow mobility. The remaining sub-sections details the proposed enhancements to PMIPv6 for ensuring session continuity during IP flow handoffs and the enhancements for enabling flow-based routing and management.

3.3.1 Architecture

The functionality to enable IP flow mobility in the EPC requires enhancements to the components providing PMIPv6-based mobility management in the EPC; these components are the PDN-GW as it contains the Local Mobility Anchor (LMA) functionality of the PMIPv6 mobility protocol and the S-GW and ePDG as it contains the Mobile Access Gateway (MAG) functionality of the PMIPv6 mobility protocol. The highlighted components in figure 3.1 illustrate the LMA and MAG functionality (refer to section 2.1.2 of chapter 2 for an overview of the LMA and MAG functionality of the PMIPv6 protocol in the EPC). The functionality required from these components for IP flow mobility will be discussed in the next sub-sections.

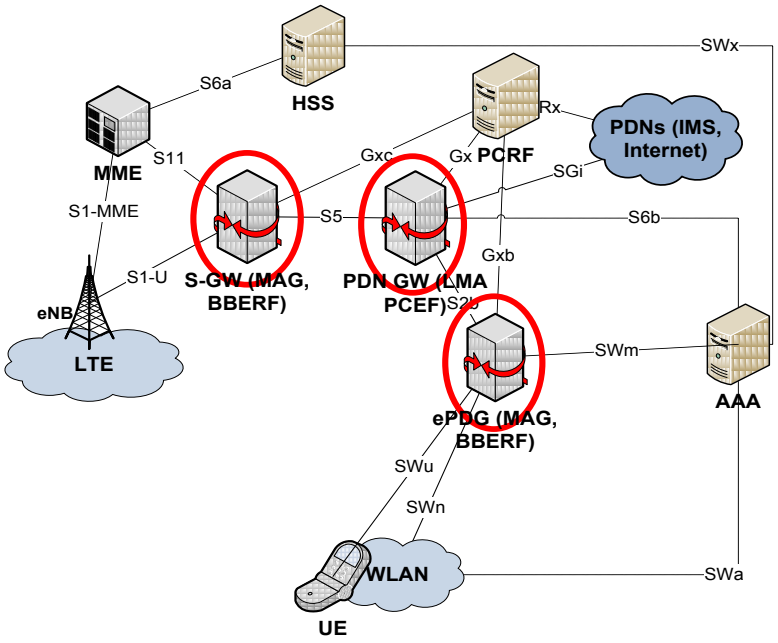

Figure 3.1: Architecture of the proposed PMIPv6 IP flow mobility solution for 3GPP's EPC

Even though the Policy and Charging Control (PCC) architecture is not within the scope of this project, it still plays a crucial role in resource management within the core network. As for the rest of the entities (i.e. Home Subscriber Server (HSS), Access Authentication and Authorisation (AAA) and Mobility Management Entity (MME)), the proposed solution imposes no further enhancements. The HSS and AAA is merely for subscription and authentication within the EPC and have no influence on the UE data path, and the MME is a control entity in charge of access gateway selection and location management i.e., it performs paging when an incoming call arrives for a UE that is in idle-mode.

3.3.2 Functionality to support multihoming

The standard PMIPv6 protocol provides basic multihoming support to the UE. When a multihomed UE attaches to the PMIPv6 domain the LMA allocates each of the interfaces a unique HNP and creates a binding cache entry for each interface. This multihoming functionality suffices for the IP flow mobility solution as it will serve as a basis upon which the rest of the IP flow mobility functionality is built. The only requirement is that UE support multihoming. Most UE nowadays come equipped with multiple network interfaces with some having the capability to use these multiple interfaces at the same time. A requirement for IP flow mobility from such devices is that the interfaces should be able to specify the same Access Point Name (APN) during initial attachment to the network. The APN can be configured manually in the UEs connectivity settings. The APN should be the same because the UEs interfaces should be attached to the same PDN-GW as this is where all the IP flow mobility functionality and information is defined for a specific UE and due to the LMA being the mobility anchor during normal handover procedures. The APN is used by the MME and ePDG during the initial attach procedure to the EPC to select the PDN-GW to attach the UE to.

3.3.3 Functionality for ensuring session continuity during IP flow handoffs

To ensure session continuity during IP flow handoffs it is proposed that the third HNP allocation scenario of the IETF standardisation body (refer to subsection 2.3.1.1.1 of chapter 2) be adopted. In this scenario, when the UE attaches a new interface to the network still keeping its previous interfaces attached, the LMA allocates a new HNP to the UE and forwards the previously assigned HNPs of the UE to the new MAG in the PBA message. This scenario is proposed as it introduces no additional signaling messages in the core network (due to the LMA sending the previously assigned HNPs in the PBA messages to the MAG) which means that it would not bring about signaling overhead.

To realise the HNP allocation scenario with PMIPv6 no recommendations were given by the IETF standardisation body on how to enhance PMIPv6 with this functionality. Hence, this section presents proposed enhancements to PMIPv6 that consists of a new binding cache entry look-up method in the LMA and a new mobility option for the PBA message. The binding cache look-up method would enable the LMA with the functionality to search for and send any additional HNPs of a particular UE in a PBA message to the MAG, and the mobility

option would enable the PBA message to transport the additional HNPs to the MAG. The MAG requires the functionality to extract and create the additional routes of the UE in its binding update list entries, which would result in the MAG being aware of all the HNPs of the UE.

To complement the session continuity enhancements, it is proposed that the UE implement the weak-host model (refer to subsection 2.3.1.1.2 of chapter 2) as it introduces the least modification to the UE and requires no enhancements on the network side.

3.3.3.1 LMA binding cache entry look-up key to extract the UEs additional HNPs

There is no functionality defined in the LMA for extracting additional binding cache entries of the UE which in turn means that the additional HNPs of the UE cannot be extracted. In order to enable the LMA to extract the additional HNPs of the UE, a new binding cache entry look-up method is proposed. The default binding cache entry look-up key used by the LMA is the UEs International Mobile Subscriber Identity (IMSI) and the APN [**19**]. For an IP flow mobility scenario the UE would have multiple interfaces attached to the network and the binding cache entries created for these interfaces would all have the same IMSI and APN. Using the default look-up key would not yield the additional binding cache entries; instead the LMA will always extract only the first entry matching the IMSI and APN. Since the binding cache entries of the UE each have a unique HNP, it is proposed that the LMA search for any additional binding cache entries of the UE using the lookup key: the UEs IMSI, APN and where the current HNP (i.e., the HNP allocated by the LMA or the HNP received in the PBU message) is different to the HNPs in the binding cache entries. This look-up key will result in the extraction of the additional binding cache entries and HNPs. Figure 3.2 shows an example of the proposed binding cache entry extraction method. From the example, the UE has three binding cache entries each having the same IMSI and APN with different HNPs (i.e., HNP1, HNP2 and HNP3). To extract the additional HNPs of the UE, the LMA uses the IMSI and APN and extracts all the binding cache entries not having the current HNP (i.e., HNP2). This results in the extraction of the first and third binding cache entries. The LMA can now extract those HNPs and send it in the PBA message to the MAG.

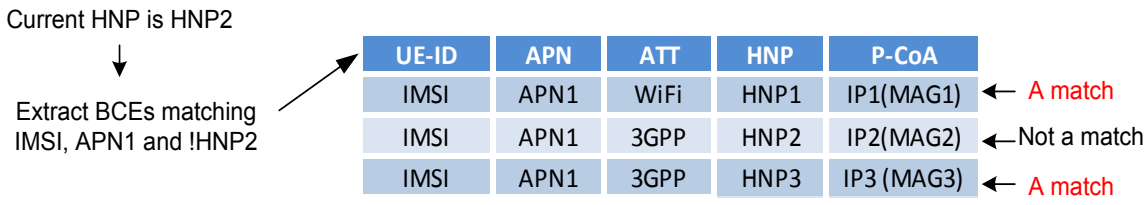

Figure 3.2: LMA extracting additional binding cache entries of the UE

3.3.3.2 Mobility option for the PBA message to transport additional HNPs to the MAG

A new mobility option, called Additional Route, is proposed for transmitting the additional HNPs in the PBA message to the access gateways (i.e., S-GW and ePDG). Mobility options form the message data parts of the PBU/PBA messages and have a specific structure according to the type of information it carries in the PBU/PBA messages. For example, the HNP and the APN each have their own standard defined mobility option to carry the HNP and APN values. The format of the PBU/PBA messages and the standardised mobility options are discussed in [**18**] and a general overview of the PBU message format is given in Appendix A.2. The format of the Additional Route mobility option is detailed in Appendix A.3.

The MAG in the access gateways only requires the functionality to extract this Additional Route mobility option from the PBA message and create additional binding update list entries for the HNPs received. The MAG would then be able to route any packets addressed to the UE since it would be aware of all the HNPs of the UE.

3.3.4 Functionality to enable flow-based routing and IP flow management

To enable flow-based routing and IP flow information management with the PMIPv6 protocol the proposed enhancements adopts a similar concept to the IETF, as discussed in section 2.3.1.2 of chapter 2. The solution allows the creation of flow bindings in the LMA functionality in the PDN-GW. A flow binding is the association between a routing filter (i.e., routing filters are defined in section 2.2.1.2 of chapter 2) and a HNP of the UE. Due to the HNP allocation scenario adopted in section 3.3.2.2 above, each binding cache entry maintained by the LMA for the UE will have a unique HNP pointing to a specific access gateway (and access network). Associating a routing filter to a HNP will enable redirecting an IP flow to a particular P-CoA (which indicates a particular access gateway) and hence

access network. The creation and management of flow bindings are performed by the UE, since the UE is aware of the end-user preferences and is aware of the access networks in its vicinity and its current interface connectivity state (i.e., whether it is attached to the access network where the IP flows are to be moved).

The proposed flow binding mechanism requires the LMA to have the functionality to store and be able to manipulate (i.e., create, modify or delete) the flow bindings as this allows rules to be set for a particular IP flow and indicate which access network the IP flow should be routed to; this functionality enables IP flow information management. The LMA also requires the functionality to identify and match packets to routing filters for the purposes of classifying the packets and then routing the packets according to the flow binding; this functionality enables flow-based routing in the LMA. Since the flow bindings is created and manipulated based on UE requests, the flow binding information needs to be sent using the PBU message to the LMA; hence the PBU message requires enhancement. The flow binding information consists of the routing filter and the HNP to which the routing filter should be associated with. The MAG requires the functionality to send the flow binding information in the PBU messages to the LMA.

The flow binding scheme consists of an additional list for storing the flow bindings and additional packet processing logic that would enable the LMA to perform flow-based routing. To transport the flow binding information a new mobility option, called Routing Rule is proposed.

3.3.4.1 Flow binding list

The LMA is enhanced to store the flow bindings of the UE in a list of entries called flow binding list. The flow binding list is stored separately from the binding cache and is associated to every binding cache entry of the UE. This simplifies the binding cache entry structure and avoids having to create duplicate flow bindings for each binding cache entry. The flow binding list entry contains the UEs HNPs and the routing filters associated to those HNPs. An example of a LMA supporting the flow binding enhancement is shown in figure 3.3. In the illustrated example, two binding cache entries of a particular UE are shown where each entry is associated to the UEs flow binding list.

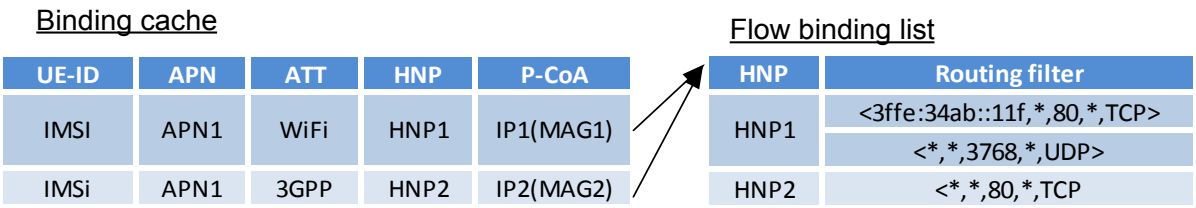

Figure 3.3: Binding cache entries and flow binding list of an UE in the LMA

3.3.4.2 Enhanced packet processing in the LMA for flow-based routing

It is proposed that for flow-based routing the LMA use the routing filters in the flow binding list during packet processing to determine the forwarding path of the downlink packets. The standard procedure at the LMA during packet processing is such that when downlink packets arrive for the UE, the LMA extracts the packet"s header and search for a binding cache entry matching the HNP of the destination IP address of the packet. If the LMA finds a binding cache entry it forwards the packet to the P-CoA (which indicates the access gateway) of the binding cache entry or drop the packet if no binding cache entry can be determined. Instead of forwarding the packets to the P-CoA immediately after determining the binding cache entry, it is recommended that the LMA first match the packet header to the routing filters in the flow binding list (this action would result in the classification of the packets) and then forward the packets to the P-CoA corresponding to the HNP of the matched routing filter. For instance, referring to the example binding cache and flow binding list in figure 3.3, if a downlink packet arrives at the LMA with a source port equal to 3768 and use UDP as the transport protocol the LMA would send the packet to the MAG1 as this is the access gateway corresponding to HNP1 of the flow binding.

3.3.4.3 Mobility option for the PBU message to transport the flow binding information

In order to send the routing filters to the LMA, a new mobility option is proposed for the PBU message, called Routing Rule mobility option. The format of the mobility option is detailed in Appendix A.4, and consists of fields for containing the routing filters and HNP and has flags to indicate to the LMA whether the mobility option is a request for the creation, modification or removal of a flow binding. The mobility option would also enable the LMA to indicate the result of the request to the MAG i.e., whether the request was successful or unsuccessful. Adopting the Routing Rule mobility option would require the LMA to have

functionality that would enable it to process the flow binding information in the option and be able to add the option to a PBA message with the status set to inform the MAG of the outcomes. The MAG would require functionality that would enable it to populate the option with the flow binding information and add the option to the PBU message.

3.4 Discussion

This chapter discussed the functional requirements for designing an IP flow mobility solution and discussed certain considerations that need to be taken into account during the design process. Thereafter, the proposed IP flow mobility scheme was described that includes enhancements to the PMIPv6 mobility functionality in the EPC for enabling session continuity during IP flow handoff and for enabling flow-based routing and IP flow information management. These proposed enhancements satisfy the design functional requirements set out at the beginning of the chapter. With regard to the design considerations, the enhancements proposed for session continuity imposes no additional signaling in the EPC network and has a minimal impact on the UE, and the enhancements proposed for flow-based routing and IP flow information management also imposes no additional signaling messages. However, the enhancements do impose additional execution stages to the packet processing and mobility message processing performed by the PDN-GW/LMA that could affect the performance of the EPC network. Thus, the chapters in the rest of this dissertation aim to firstly, analyse the feasibility of the IP flow mobility scheme using a real emulated EPC environment, and then evaluate the performance of the scheme to determine how it would affect the network performance and the end-user QoE.

Chapter 4

Design and Implementation of an Evaluation Framework

The previous chapter presented the enhancements to the PMIPv6 mobility functionality of 3GPPs EPC to enable IP flow mobility. In order to verify the feasibility of the proposed functionality in typical deployment scenarios, it needs to be implemented in a practical testbed that would allow performing evaluations to show the performance of the functionality in a realistic environment. The IP flow mobility functionality could be developed in a simulation environment (as was done in the related literature), but simulations are usually subjected to assumptions that, though theoretically accurate, do not take all the variables of a practical network into consideration. A testbed environment surmounts the limitations of simulation environments as more realistic analysis can be performed and results obtained.

Developing a standards compliant EPC testbed environment and incorporating the proposed IP flow mobility scheme would prove to be difficult due to the complexity of the EPC and the time required for completing such an environment for research purposes. Hence, the Centre for Broadband Networks at the University of Cape Town (UCT) [45] has acquired a licensed (i.e. not open source) EPC emulation environment, the OpenEPC [24]. The OpenEPC, developed by the Fraunhofer Institute for Open Communications Systems FOKUS [46] in Berlin is a complete prototype implementation of the 3GPP release 9 EPC standards. The OpenEPC includes all the components of the EPC and enables all-IP connectivity over 3GPP accesses (e.g. LTE, WCDMA, etc) and non-3GPP accesses (e.g. Wi-Fi, etc). The

OpenEPC comes as a software toolkit that is highly configurable and extensible in that it allows the nodes to be configured to match the needs for testing only some functional components and it allows the prototyping of new network features on the EPC. The OpenEPC software toolkit is thus used for developing a physical testbed environment (hereon out referred to as an evaluation framework) on which the proposed IP flow mobility scheme is implemented and the feasibility verified.

The rest of this chapter details the functional requirements and components necessary for developing the evaluation framework. An overview of the architecture of the evaluation framework is then discussed. This is followed by a discussion on the design and implementation of the proposed IP flow mobility scheme, highlighting the extensions made to the OpenEPC toolkit components.

4.1 Requirements of the Evaluation Framework

In order to implement and verify the proposed IP flow mobility scheme in a suitable practical environment, a number of components and functionalities are required to develop such an environment.

An important functionality required is the support for mobility with the PMIPv6 protocol, as the proposed IP flow mobility scheme discussed in chapter 3 is realised by enhancing PMIPv6. The mobility functionality should also allow the UEs to attach to more than one access network simultaneously i.e., the mobility entities should support multihoming. Multihoming is a requirement for IP flow mobility. Any PMIPv6 implementation should provide multihoming capabilities, since it is supported by the standard PMIPv6 mobility protocol.

The EPC entities requiring enhancements for the proposed IP flow mobility scheme are the PDN-GW, S-GW and ePDG as these are the components containing the PMIPv6 mobility functionality in the EPC. To conform to a typical MNO implementation and to ensure that the results obtained during the performance evaluation accurately reflects the performance of a real EPC deployment, these entities cannot operate without the rest of the EPC entities i.e., HSS, AAA, PCC and Mobility Management Entity (MME); a fully functional EPC architecture is thus necessary for the implementation and verification of the proposed scheme.

For evaluating the performance of the IP flow mobility functionality it should be possible to establish suitable services through the EPC network. The services are representative of the

IP flows and could be both UDP and TCP based services. UDP based services represents real-time services like VoIP, video conferencing and IPTV, whereas TCP based services like file transfer, email and peer-to-peer (p2p) [42] represent non real-time services. UDP based services are not offloaded from the LTE network due to the stringent QoS requirements of these services. TCP based services are the most likely services to be offloaded to WLAN as these services have less stringent QoS requirements. To orchestrate the different types of IP flows, a Hypertext Transfer Protocol (HTTP) [47] proxy server and a video streaming server is required. The HTTP proxy server is used for establishing connections to the internet for YouTube TCP traffic and the video streaming server is used for establishing video conferencing UDP traffic.

In order to initiate and terminate services over EPC core network, and for sending attachment and handover attach events to the EPC network, UE components are needed. The UE should also have a communication means for accessing the services on the servers and to attach to the EPC network. Thus, the final components required are access network technologies providing the communication between the UE and the EPC network; the access networks of interest are LTE and WLAN, as these are the networks for which the IP flow mobility scheme is designed.

4.2 Software and architecture of the evaluation framework

The OpenEPC is based on a flexible and powerful programming framework, completely written in C programming language and is designed for developing software-based operator core network functionality and components [24]. The architecture of the evaluation framework is illustrated in figure 4.1.

The toolkit provides all the EPC components set out in the requirements section and a complete implementation of the PMIPv6 protocol. Standard radio components like LTE and 3G base-stations can be integrated with the OpenEPC for allowing experimentations in realistic radio conditions [24]. However, due to the cost and licensing requirements associated with deploying real LTE or 3G base stations for academic purposes, the OpenEPC also provides radio emulation nodes (e.g. eNodeB) that emulates the functionalities of the real radio base-stations. Unlicensed spectrum technologies like Wi-Fi access points are also supported for realising connectivity to non-3GPP access networks. User equipment implementations are also provided; the UEs can select access networks, evaluate radio conditions, perform location based handovers and initiate services. For service orchestration,

the toolkit provides an Internet gateway for internet connectivity and a Media Delivery Function (MDF) which acts as a video streaming server for real-time VoD services. The Internet gateway is a Squid [48] HTTP proxy server. The Squid HTTP proxy server is implementable on most operating systems and is licensed under the GNU General Public License (GPL) [49]. Squid is not developed by the Fraunhofer FOKUS, but is rather interworked in the OpenEPC toolkit; the reader is referred to [48] for more information regarding Squid. The video streaming server uses UDP as the transport protocol and is able to transmit video at variable bit rates. The bit rate used for a particular video stream is based on the resources (e.g. bandwidth) that the Policy and Charging Rules Function (PCRF) [11] of the Policy and Charging Control (PCC) [11] architecture is able to establish in the access gateways for the video stream (Appendix A.1 gives a brief description of the PCC architecture, refer to [11] for a complete description of the PCC architecture and its functionality). For instance, when a video stream is requested, the video server interacts with the PCRF to request for resources (e.g. bandwidth). Depending on the access network load the PCRF replies with a confirmation on whether the resources requested is available and the video server adapts the video stream according to the resources allocated from the PCRF. An overview of the video streaming server and its interconnection with the PCRF architecture is given in Appendix C.1. In order for the UE to establish a video stream from the MDF, the UE incorporates a software tool called Multimedia Open InterNet Services and Telecommunication EnviRonment (myMONSTER) [50]. The myMONSTER tool is a Session Initiation Protocol (SIP) [51] client used for communicating with the MDF; refer to Appendix C.2 for an overview of the myMONSTER tool and an example of how the video stream is established. SIP is an application layer signaling protocol used for controlling multimedia sessions over IP networks. SIP defines the messages that are sent between communication peers for establishing and terminating (and other elements) a session. The MDF and UE are the SIP communication peers in the OpenEPC. The reader is referred to the RFC defined in [51] for an in-depth description of the SIP protocol.

The testbed comprises of a PDN-GW, MME, S-GW, ePDG, eNodeB and Enablers machines arranged in a single administrative domain (representing a core network of a single mobile network operator) and divided into five subnets. All the EPC components are installed on Linux Desktop Computers with the system specifications as listed in table B.1 of Appendix B. The components are connected through Ethernet cables to five Ethernet switches (indicated by net_a, net_b, net_c, net_d and mgmt). The maximum link speed between any two machines is 100Mbps.

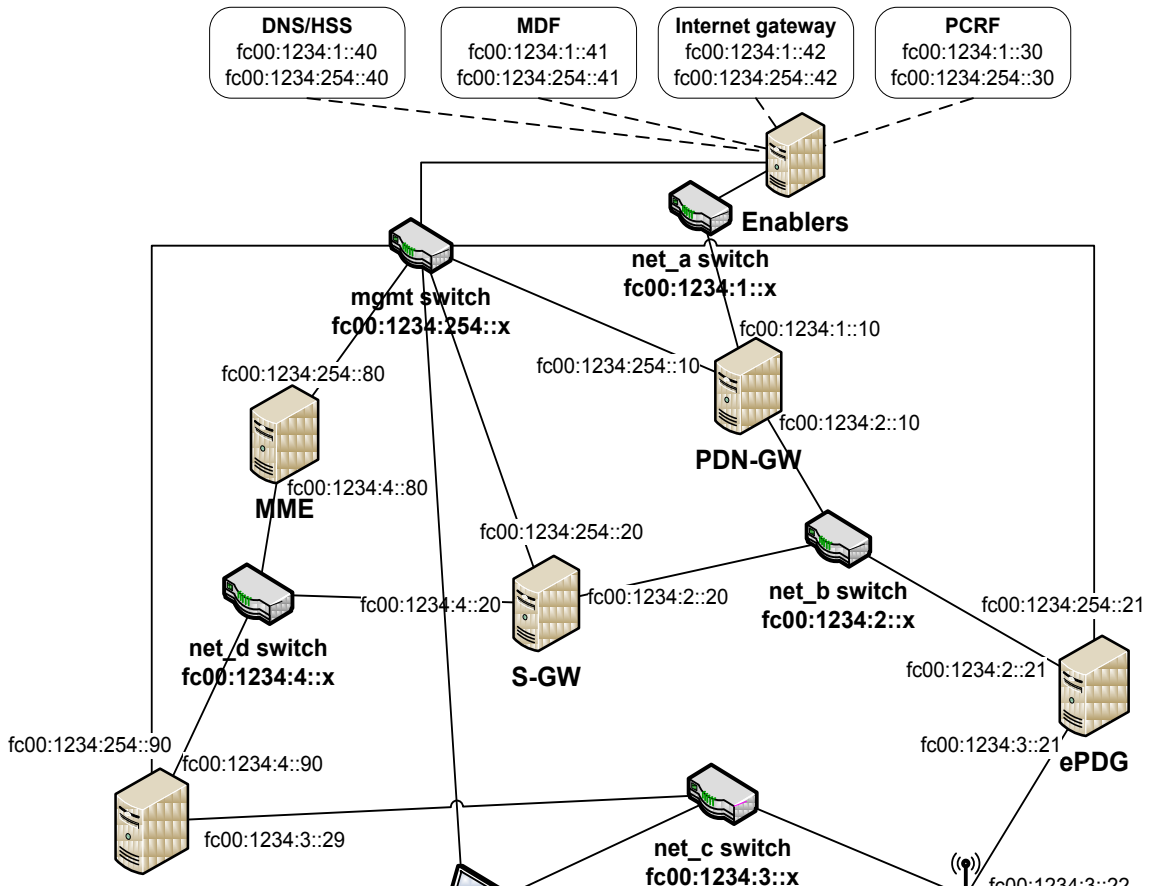

Figure 4.1: Architecture of the evaluation framework

The first subnet in the architecture is defined between the PDN-GW and the Enablers and is interconnected with the net_a Ethernet switch. The net_a switch represents the IP backhaul of the network operator. The Enablers machine houses six individual entities: the Domain Name Server (DNS) for address resolution, the Home Subscriber Server (HSS) for end-user subscription management, the MDF, the internet gateway and the PCRF that is in charge of QoS rules provisioning to the PDN-GW and access gateways. The second subnet is defined between the PDN-GW, S-GW and ePDG machines with the net_b ethernet switch representing the operator‟s core backhaul network. The third subnet is defined between the UE, eNodeB and ePDG machines with net_c representing the operator‟s access backhaul network. The fourth subnet is defined between the MME, eNodeB and S-GW and is interconnected with net_d Ethernet switch that represents the GTP control signaling network. All the machines in the architecture are connected to a management (mgmt) Ethernet switch; this represents the final subnet of the architecture. The management switch is used by the

entities for DNS queries, HSS signaling and for debugging the individual testbed components. An 802.11 access point is connected to the net_c Ethernet switch and ePDG for providing wireless connectivity to the EPC. Table B.2 in Appendix B lists all the hardware used in the testbed.

The framework enables the UE to establish services and perform handoffs between the LTE and WLAN network. However, the UE is implemented on a stationary Linux machine, thus the UE attachment and handoffs are triggerred by bringing up the respective interfaces on the UE. The next sections in this chapter details the software and the enhancements made to the OpenEPC toolkit for IP flow mobility (only the enhanced nodes are detailed). These enhancements are implemented in the respective EPC machines in the architecture described above.

4.3 Detailed design of the IP flow mobility functionality and development using the OpenEPC toolkit

The OpenEPC toolkit provides a modular design for simplifying the software and enabling the use of a single module in multiple components. Each component within the OpenEPC toolkit has a set of modules on which its functionality is dependant. Modules in the PDN-GW, S-GW, ePDG and the UE are enhanced to support IP flow mobility. Moreover, the OpenEPC has a limitation in that the PMIPv6 implementation and UE does not support multihoming. Thus, before the IP flow mobility enhancements of chapter 3 are developed in the OpenEPC toolkit, the multihoming limitation is also addressed since IP flow mobility requires multihoming functionality on the UE and the network. The sub-sections that follow discuss enhancements made to the components.

4.3.1 The OpenEPC PMIPv6 mobility enablers

The PMIPv6 mobility enablers in the OpenEPC comprise the LMA and MAG components. The LMA is collocated with the Policy and Charging Enforcement Function (PCEF) of the PCC in the PDN-GW and the MAG is collocated with the Bearer Binding and Event Reporting Function (BBERF) of the PCC in the access network gateways (i.e. the S-GW and the ePDG, etc). A handover in OpenEPC works as an attachment to the new access network followed by a detachment from the old access network. Figures 4.2 show a simplified version of a handover operation in the OpenEPC, where the UE is firstly attached to the source access

network (step 0) and then performs the attach procedure to the target access network (steps 1-8). The attach procedure to the target access network serves as a handover trigger to the LMA; the LMA allocates the same IP address to the UE for session continuity. After step 8 the UE is attached to the target access network and releases the previous connection to the source access network (steps 9-12).

The MAGs receive information and address requests from the UE via the Enhanced Host Configuration Protocol (EHCP) signalling (sub-section 4.4.1.2 below gives a brief explanation on EHCP). This information is then relayed to the LMA using PBU message, where IP allocation is then performed. The response is then sent to the UE and for at least one UE served by the LMA, a tunnel is constructed.

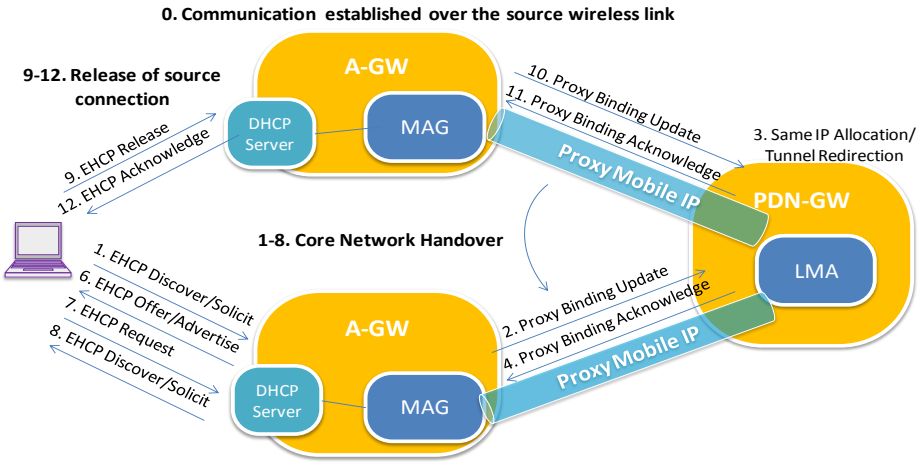

Figure 4.2: Handover with the OpenEPC PMIP mobility enablers

4.3.1.1 PDN-GW/LMA

Figure 4.3 illustrate the interworking between the modules making up the PDN-GW functionality. From figure 4.3, the LMA consists of the pmip_lma, mobile_ip, ip_allocation, routing, routing_raw and routing_encap modules. The pmip_lma module provides the LMA functionality itself. This module performs all the standard LMA procedures like the PBU message processing, PBA message creation, binding cache management and tunnel management procedures. The mobile_ip module provides the MIP protocol stack functionality in the PDN-GW. It defines all the MIP message and mobility option formats (e.g. PBU, PBA, HNP, etc.) and functions to encode and decode the messages and mobility options. The ip_allocation is used by the LMA for allocating IP addresses during the initial attach and handover attach procedures of the UE. Three pools of IP addresses are maintained

by the ip_allocation module: an IPv4, IPv6 and IPv6 HNP pool. The LMA performs its own processing of data packets in order to control forwarding and tunnel management. Packet processing and routing is achieved through a routing module. The routing module contains packet handler procedures for both IPv4 and IPv6 packets that allows high level packet processing separately from the normal Linux kernel packet processing procedures. The routing module interacts with the routing_encap and routing raw modules: The routing_encap module provides tunnelling functionality on the S5, S2a/S2b interfaces between the PDNGW and S-GW and ePDG, and the routing_raw module is used to send and receive packets using raw sockets on the SGi interface between the PDN-GW and the PDNs. Raw sockets means that the packets is not processed through the normal Linux kernel packet processing procedures but rather the packets can be passed to the application requiring the packet (in this case the packet handler in the routing module).

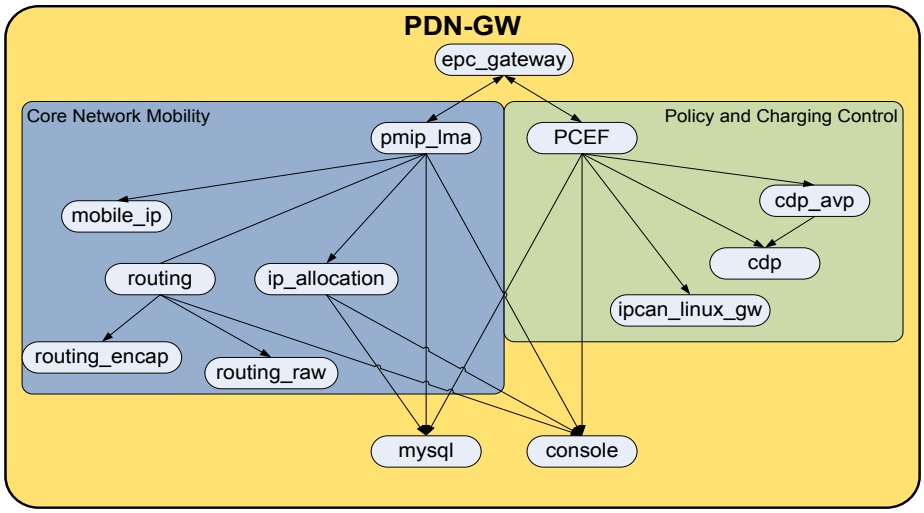

Figure 4.3: The module structure of the PDN-GW component

Multihoming support in the LMA is enabled by modifying the ip_allocation and pmip_lma modules. The standard operation of the pmip_lma module is such that when a PBU message is received from a MAG that the UE is attached to, the pmip_lma concludes that the PBU message is received as a handover request and performs the handover to the new MAG. This standard operation is modified and the pmip_lma module is enhanced to treat the second UE connection as an initial attach request and not as a handover request. The ip_allocation module is enhanced to deprecate allocating the same HoA/HNP during subsequent attaches made by the same UE. The enhancement is made because the LMA performs the attach procedure and requests an IP address from the ip_allocation module for every UE attach

request. The ip_allocation module searches for an IP address belonging to the IMSI of the UE, as it maintains state in a database as to what IP addresses it had previously assigned to the UE. If an IP address is found the ip_allocation module returns that IP address to the LMA who in turn allocates the address the UE. After the enhancements made to the pmip_lma and ip_allocation modules, the UEs second interface attachment is considered as an initial attachment and a different IP address is allocated to this interface. The UE will also have a different binding cache entry and routing entry for each of its attached interfaces.

To enable the IP flow mobility functionality proposed in chapter 3, modifications are made to the pmip_lma, the mobile_ip and the routing modules. The PBA creation procedure in the pmip_lma module is enhanced with additional execution stages in order to enable the LMA to search for and send any additional HNPs belonging to a particular UE in a PBA message. (i.e., the functionality proposed in section 3.3.3.1). Enhancing the PBA creation procedure does not affect any other LMA procedure since it is the last procedure performed. The additional execution stages are detailed in Appendix D.1. The pmip_lma is also enhanced with a new list structure (i.e., the flow binding list of section 3.3.4.1) to store the flow-bindings of the UE. In order for the LMA to create, modify or delete entries in the flow binding list and to process the Routing Rule mobility options, requires enhancements to the default PBU message processing procedure. To enable this functionality the PBU processing procedure is enhanced to process routing rule mobility options according to the method detailed in Appendix D.2.

For flow-based routing the packet processing enhancements of section 3.3.4.2 are developed in the packet handler function of the routing module. The packet handler was enhanced to extract the complete IP 5-tuple from the incoming packet‟s header, since this was not performed in the standard OpenEPC routing module. The 5-tuple is then matched to the routing filters associated to the UE in order to find the gateway IP address (the Proxy care-of address (P-CoA)) to send the packet to. The routing module maintains separate routing tables for the UEs (this is in addition to the binding cache maintained by the LMA). There exists a destination table for downlink packets and a source table for uplink packets. Each binding cache entry maintained by the LMA has an underlying routing entry. A typical routing entry contains the UE‟s HoA/HNP, P-CoA, tunnel endpoint identification, and an indication of the extensions i.e., whether the packet arrived on the downlink or on the uplink PDN-GW extension. The UE‟s routing entry is linked with its binding cache entry through the HoA/HNP. Due to the separate routing state maintained for the UE, only the routing table is used to route the IP packet, since it contains the gateway IP address and the UE‟s IP

address. Thus, when a downlink packet matches a routing filter, the HoA/HNP corresponding to the routing filter is used to search for the UE"s routing entry, the packet is then sent to the gateway IP address in the routing entry. Appendix D.3 details the packet processing logic for flow based routing.

The mobile_ip module is enhanced with the additional mobility options of Appendix A.2 and A.4. The formats of the mobility options, the Type parameter and functions enabling the encoding and decoding of the mobility options is defined in this module. These functions are used by the LMA during PBU processing and PBA creation procedures.

4.3.1.2 S-GW and ePDG

The module structure of the S-GW and ePDG is shown in figures 4.4 and 4.5 respectively. In both the gateways, the MAG functionality comprises of the pmip_mag, mobile_ip, routing, routing_encap, routing_raw, routing, ehcp_daemon and ehcp_messaging modules. The MAG in the S-GW uses a GTP_comm (GTP communication) module instead of the routing_raw module. The GTP_comm module provides the communication functionality for the GTP protocol, since the GTP control (GTP-C) protocol is used for communicating with the eNodeB and MME entities. The mobile_ip, routing, routing_encap and routing_raw are the same modules as implemented in the LMA (this is enabled due the modular design of the OpenEPC).

The pmip_mag module provides the MAG functionality where all the MAG procedures are defined. The routing module has the same functionality as previously described. The routing_encap module provides tunnelling functionality on the S5, S2a and S2b reference points towards the PDN-GW and the routing_raw module is used for routing raw packets between the ePDG and the UE in non-3GPP accesses. The Fraunhofer FOKUS developed a protocol called EHCP that is specific to the OpenEPC for enabling communication between the UE and core network nodes. EHCP is a modified version of the IETF Dynamic Host Configuration Protocol (DHCP) [52] [53]. DHCP is used for stateful address configuration and consists of a DHCP server in the network which allocates IP addresses to end-users. The EHCP comprises of a ehcp_messaging module containing the EHCP message stack and a ehcp_daemon module providing the EHCP server functionality. EHCP operates somewhat differently to the DHCP protocol since in the OpenEPC the PDN-GW is in charge of allocating IP addresses to end-users, not the EHCP server. EHCP is merely used for relaying IP address configuration information from the PDN-GW to the UE.

To enable the MAG with the IP flow mobility functionality proposed in chapter 3, the pmip_mag and mobile_ip modules are enhanced. The enhancements to the modules apply to all the MAGs, meaning that both the S-GW and ePDG will received the same modifications. The extensions applied to the mobile_ip module of the LMA component in 4.3.1.1 above are applied to the mobile_ip module in the MAG. The pmip_mag module providing the PBA processing functionality of the MAG is enhanced (section 3.3.2.2 of chapter 3) to process the Additional Route mobility option. The enhancements enable the MAG to create a separate binding update list entry for HNP received and also create a routing entry in the routing table maintained by the routing module. The MAG does not require any enhancements for multihoming. The detailed procedure for extracting the additional HNPs is outlined in Appendix D.4

A requirement of the MAG is that it should be able to add the flow binding information in a PBU message for transport to the LMA, thus a new function was created to take in the routing filters and HNP as input parameters, and call the PBU message creation procedure to add the information. The PBU message creation procedure uses the enhancements in the mobile_ip module to add the information in the Routing Rule mobility option and append it to the PBU message.

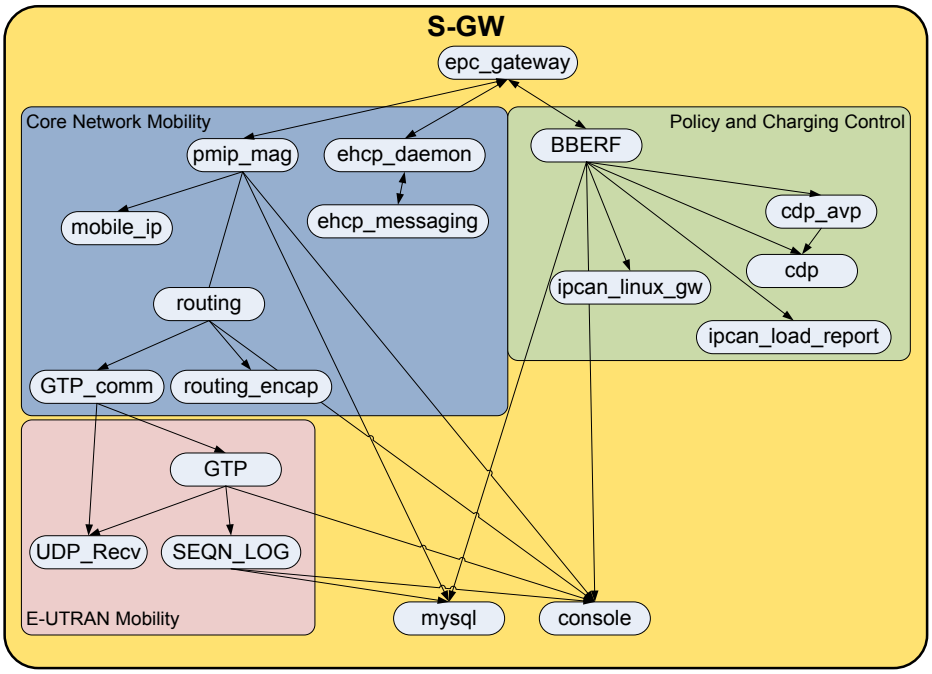

Figure 4.4: The module structure of the S-GW component

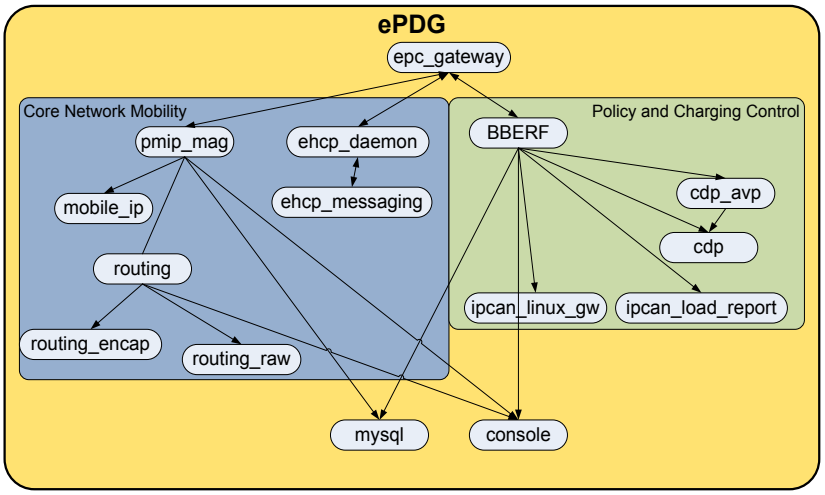

Figure 4.5: The module structure of the ePDG component

4.3.2 User Equipment

The UE contains an ehcp_messaging module and a Mobility Manager (MM) module. The MM is in charge of orchestrating the UE‟s attachment/detachment events by sending EHCP message to the OpenEPC and is in charge of configuring the UE‟s interfaces with the IP addresses received from the PDN-GW and manages the internal routing table of the UE. The routing of the UE is completely based on the Linux Kernel routing mechanisms. The attachment and detachment events on the UE can be manually controlled through an end-user Graphical User Interface (GUI) or through using command line in Linux terminal. The GUI is used for the attachment and detachment events in the framework; an overview of the MM GUI is given in Appendix C.3.

A requirement of IP flow mobility is that the UE be multihoming capable, meaning that the UE is able to attach multiple interfaces to the network and simultaneously send and receive data through the interfaces. The UE implementation on the OpenEPC toolkit does not support multihoming; the UE is restricted to attaching only one interface at a time to the OpenEPC. This restriction is due to the lack of multihoming support of the MM module; when the UE is attaching a second interface the MM concludes that the UE is handing over when the access network technology type of the new interface is different to the attached interface. The MM detaches and switches off the previous interface. The lack of multihoming support by the MM module is solved by enabling the MM to keep the previous interface active and leaving the IP address configuration and routing state of the previous interface intact. When a new interface is attaching, the interface is configured with a new IP address and a new route is entered in the Linux host routing table.

Since the UE is implemented on a Linux based operating system (refer to table B.1 in Appendix B), the weak host model required to complement session continuity is set by default in the Linux kernel. This is however only for Linux-2-6 kernels onward and is enabled for both IPv4 and IPv6 interfaces.

4.4 Limitations of the prototype implementation

The IP flow mobility prototype developed with the OpenEPC is a coarse implementation and is by no means representative of a complete IP flow mobility solution. In this dissertation the prototype is merely developed in order to evaluate the feasibility and performance of the proposed IP flow mobility mechanisms. The prototype has a few limitations, i.e., there are no intelligent congestion/bandwidth monitoring tools that can automatically trigger IP flow mobility in the network if a certain link/access network gets congested. Instead, IP flow mobility is manually triggered through the Linux terminal and is assumed to be based on end-user preferences (e.g. cost). A simple function was written to trigger the IP flow mobility procedures in the OpenEPC. The function allows sending a PBU message with a routing rule to the PDN-GW through the Linux terminal after the UE has attached both interfaces to the network. The function can set the intension of the routing rule i.e., whether it is to add, modify or delete a flow binding at the PDN-GW. This simplistic method of triggering IP flow mobility is deemed to be sufficient to test the procedures and feasibility of the proposed IP flow mobility solution. Future implementations can refine this method.

The prototype also has the limitation that TCP IP flow handoffs causes non-optimal routing of the TCP downlink packets and the TCP acknowledgements sent from the UE. For instance, when a TCP IP flow is moved to a new interface the downlink TCP packets are routed to the new interface while the UE sends the TCP packet acknowledge through the previous interface. This limitation is due to the lack of higher layer routing table manipulation in the UE (as in the LMA with the packet handler function) and due to the proposed IP flow mobility solution only accounting for downlink IP flows. To overcome this limitation when ever a TCP IP flow is moved to a new interface, a routing rule is manually set in the UE‟s routing table. This routing rule influences the outgoing interface through which the IP packets matching a certain source address is routed and is based on an open source Linux routing package called netfilter [54].

4.5 Discussion

This chapter has detailed the architecture of the evaluation framework and software enhancements made to the OpenEPC toolkit in order to realise the proposed IP flow mobility solution. The evaluation framework comprises of all the EPC elements, a UE, an emulated eNodeB and a real commercially available Wi-Fi access point. The framework allows UEs to request service by connecting to a Media Delivery Function for real-time non-interactive video streaming or an HTTP proxy for Internet.

The framework enables the evaluation of the proposed IP flow mobility solution in a practical environment; this ensures that results obtained from the performance evaluation are a realistic representation of an IP flow mobility deployment in the real MNOs EPC network.

The next chapter analyzes the results obtained from experiments performed on the testbed.

Chapter 5

Performance Evaluation

The previous chapters detailed the proposed PMIPv6 enhancements to support IP flow mobility functionality in the EPC, and detailed the implementation of the solution in a real emulated EPC testbed. This chapter provides an experimental analysis of the proposed IP flow mobility functionality. The testbed is used to subject the IP flow mobility functionality through various tests for demonstrating proof of concept and to evaluate the effectiveness of the proposed solution.

For demonstrating proof of concept, tests are performed to validate the session continuity and the IP flow information management and flow-based routing functionalities presented in chapter 3. Additionally a use case scenario is analysed to show the impact IP flow mobility functionality could have on application performance when adopted in the EPC. The applications considered in the use case scenario are Video on demand (VoD) and file transfer. The results obtained from the use case scenario aim to show that IP flow mobility functionality could enhance application performance and in turn the end-user experience.

Metrics investigated for evaluating the proposed IP flow mobility functionality are those that could be affected by the functionality and in turn have an effect on the end-user quality of experience, the EPC network utilisation or overall efficiency. The metrics measured are IP flow handover latency, the throughput and packet processing delay of the PDN-GW and the signaling overhead incurred between the EPC network entities due to an IP flow handoff. The definition and motivation behind the metrics measured is discussed in the respective sections in the performance evaluation section of this chapter. The solution is also evaluated on the

ability to handle load (i.e., multiple simultaneous IP flow handover requests) from a large mobile subscriber base. The results obtained from the performed evaluations aim to indicate the effectiveness of the proposed functionality, as well as the limitations in order to provide insight for future work.

5.1 Proof of concept evaluation

In this section, two tests are performed and the results analysed. The first test validates the proposed IP flow mobility functionality and the second test is to demonstrate that IP flow mobility functionality could enhance end-user experience by improving application performance. The second test comprises of a comparative study between a scenario when IP flow mobility functionality is used for WLAN offloading against the scenario where IP flow mobility is not used for offloading, but where the end-users entire traffic is moved to the WLAN access network instead.

5.1.1 Scenarios

The tests in this section consider two scenarios: The first scenario serves as the reference case that implements only the standard PMIPv6 mobility solution without any IP flow mobility mechanisms. A handover in this scenario would result in a complete handoff of all the end-users traffic which is analogous to the functionality supported by the WLAN offloading solutions pre-release 8 of the EPC (i.e., before 3GPP introduced the IP flow mobility concept). The scenario is achieved by implementing the unaltered OpenEPC toolkit in the testbed and comprises of all the machines described in chapter 4. The second scenario incorporates the proposed IP flow mobility enhancements to the PMIPv6 protocol as described in chapter 3. This scenario is achieved with the software enhancements as detailed in chapter 4 and also comprises of all the machines described in chapter 4.

To get results representing realistic results from a real MNOs network, various traffic load states (i.e., background traffic) are created within the testbed environment for both scenarios. The traffic loads are created to resemble a case where the LTE access network is congested and the WLAN access network is not congested, hence creating the need for WLAN offloading. To realise this scenario, the traffic load in the LTE access network backhaul is set at 90% of the full capacity (which is 100Mbps) and is realised by running a UDP stream with a bit-rate of 90Mbps on the link between the eNodeB and S-GW using the

Iperf [**55**] utility (an overview of Iperf is given in Appendix E.1). Background traffic is also created between the core entities i.e., the PDN-GW, S-GW and ePDG. The traffic load between the core entities is set to 30%, this is based on the assumption that the core network backhaul capacity (between the core entities) is always greater that the access backhaul capacity (between the core network and the access networks e.g. between the S-GW and eNB), because the core network interconnect many access networks and has to be able to handle to traffic generated by these accesses. The background traffic in the core is also created with an Iperf UDP stream, this time with a bit-rate of 30Mbps. Two UDP streams are created; the first stream runs on the link between the S-GW and PDN-GW and the other on the link between the ePDG and PDN-GW. The background traffic in the access backhaul of the WLAN access network is set to 10% and created with a UDP stream of 10Mbps between the ePDG and another UE device using Iperf.

5.1.2 End-user services considered in the evaluations

An end-user could have a multitude of different types of services established in the EPC network e.g., VoIP, IPTV, file transfer, browsing the internet, etc., and all in different combinations. These services are commonly based on two types of transport protocols: UDP (VoIP, IPTV) and TCP (file transfer, HTTP). For proof-of-concept testing, IP flow mobility requires at least two or more simultaneously running services at the UE. Due to the various different combinations and quantity of services that could be chosen for the tests, evaluating all of them would be time consuming. Only one combination of services is considered for the end-user: It is assumed that the end-user is running simultaneously a real-time UDP-based video streaming service and a non-real-time TCP file transfer service. A UDP and TCP-based service is chosen since it supports the basic concept of IP flow mobility i.e., offloading non-real-time traffic to WLAN while keeping real-time traffic on the LTE access network.

The video streaming service considered is an IPTV service and is realised with the MDF as described in chapter 4. The TCP file transfer is realised with the Iperf utility where the server runs in the EPC-enablers machine and the client within the UE. Downloading a file from the internet with the HTTP proxy would not show the characteristics from the testbed. Since, TCP is sensitive to Round-trip Time (RTT) and packet loss [56] [57], and the path from a download server in the Internet to the UE in the testbed would have a RTT far exceeding the RTT between the UE and the EPC-enablers machine. Packet loss could also occur within the Internet and could affect the results obtained from the tests; packet loss

results in throughput degradation of a TCP connection [57].

5.1.3 Validating the IP flow mobility mechanisms

The test performed in this section considers the second scenario as described in section 5.1.1 and the services described in section 5.1.2. To verify the effectiveness of the IP flow mobility mechanisms, for the flow-based routing and IP flow information management functionality different IP flow handoff requests are sent to LMA (i.e., a requests for creating, modifying and deleting of flow binding) in order to move the services between the UEs interfaces. If the services are successfully moved per the requests, the effectiveness of the flow-based routing and IP flow information functionality would have been verified. The session continuity mechanism would be considered effective if all the IP flows are not discontinued during the IP flow handoffs.

Figure 5.1 illustrates the traffic capture received on the LTE and WLAN interfaces at the UE. The Wireshark [58] protocol analyser tool is used to capture the IP flows on both the interfaces at the UE simultaneously (an overview of the Wireshark tool is given in Appendix E.1). The x-axis represents the time in seconds (s) of the test duration, and the y-axis represents the throughput of the two services. The UE is attached to both access networks before the services are established. At time T0 and T1 the file transfer and the video streaming service is established respectively. Both services are established across the LTE interface. The video streaming is represented with the red line and the file transfer with the black line.

At time T2 and T3, a trigger for IP flow mobility is sent to the PDN-GW/LMA to offload the file download and video stream to the WLAN interface, respectively. The respective triggers for IP flow mobility is a PBU message containing the Routing rule mobility option with the routing filter identifying the file download and video streaming IP flow. The request in the Routing Rule mobility option is for the creation of the flow bindings. After the LMA creates the flow bindings, the file download and video streaming IP flows are received on the WLAN interface (for the file download a routing rule in the UE had to be installed manually in order for the UE to send the TCP acknowledgement messages through the WLAN interface, for UDP-based applications like the video stream the routing policy at the UE is not necessary as the streaming is one-way traffic (no uplink acknowledgement are required)). Since the PDN-GW/LMA successfully re-directed the file download IP flow to the WLAN access after receiving the IP flow mobility information, indicates that the LMA

had to determine that the mobility option in the PBU is for a request to create a flow-binding, extract the flow information from the option, create the flow bindings and match the downlink packets to the routing filters in order to forward the packets to the WLAN access. The results thus indicate the effectiveness of the flow-based routing mechanism, since the LMA is able to create flow bindings and identify both UDP and TCP based traffic and route it based on the flow bindings created in the flow binding list.

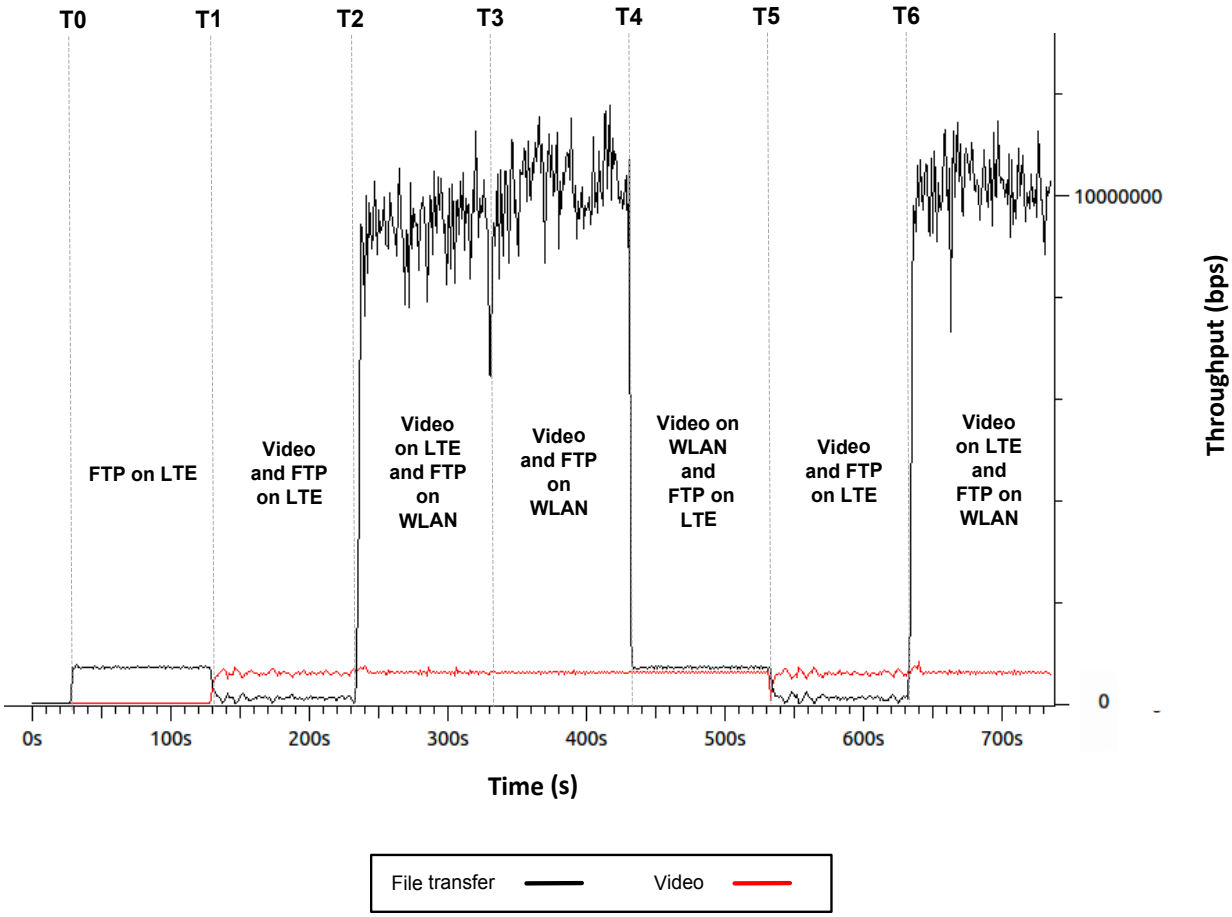

Figure 5.1: Validating the IP flow mobility functionality

Further testing is performed, to determine whether the LMA can update and delete a flow binding. Thus, at time T4 an IP flow mobility trigger is sent to the PDN-GW in order to request to update the file download flow bindings in order re-direct it back to the LTE access. After the LMA updates the previous flow binding, the UE receives the file download on the LTE interface. At time T5, an IP flow mobility trigger is sent to the PDN-GW to request to delete the flow binding of the video streaming IP flow. Since the video stream was initially

established through the LTE access, deleting the flow binding would result in the LMA routing the video stream according to the binding cache entry; this is evident from the figure. The last IP flow mobility trigger sent was another update flow binding request for moving the file download to the WLAN access again.

Throughout the test the results indicate that neither the video streaming nor the file transfer are discontinued during the IP flow handoff. Thus, verifying the proposed session continuity mechanism.

5.1.4 Enhancing the end-user quality of experience of real-time and non-real-time services

To show that IP flow mobility could improve the end-user experience, the approach taken in this section is to quantitatively measure and compare key performance indicators (KPIs) of the video and file transfer service that impact the end-users‟ perception of quality, for the two scenarios described in 5.1.1.

Services like IPTV and file transfer has unique key performance indicators that must be measured independently. File transfer is usually a best-effort service and is intolerant to packet loss and latency. End-users perceive poor quality if, for instance, the speed of their file transfer is slow i.e., taking twenty minutes to download a 1 megabyte file. The most widely used KPIs for file transfer services are goodput. Goodput is defined as the amount of useful data that can be processed by the application running in the UE within a given period of time [**59**]. Goodput is similar to throughput, but measurement excludes any packet headers, information lost or errored in transit and any duplicate transmissions or retransmissions [59]. Video services are sensitive to latency and packet loss. For instance, lost packets in a video stream means that complete video frames are lost and thus resulting in video image distortion that is perceptible to end-users. KPIs for video services are typically latency and packet loss. The KPIs measured in the proof of concept test is the packet loss ratio experienced by the IPTV service and the goodput experienced by the file transfer as perceived at the UE. Packet loss ratio is defined as the number of packets lost per total packets sent between the PDN-GW and UE. With regard to the packet loss ratio measurements of scenario 1, video streaming services like IPTV have certain QoS requirements that need to be met in order to be of acceptable quality to the end-user. 3GPP recommended that a maximum packet loss ratio of 1% [60] [11] should not be exceeded between the UE and PDN-GW for video services. Thus, in both the scenarios there is also a comparison made to the recommended

packet loss ratio in order determine whether the functionalities meet the requirement.

5.1.4.1 Experimental procedure

The packet loss ratio is measured as follows: In the EPC-enablers all the downlink video packets are captured with the Wireshark protocol analyser tool, and in the UE all the received video packets are captured on both network interface cards. The packet loss ratio is then calculated by first determining the total packets lost (i.e., total packets sent by the MDF minus the total packets received by the UE), and then dividing the result by the total packets sent by the MDF. The goodput of the file transfer is obtained from the Iperf client running in the UE. At the UE, Iperf reports the goodput of the stream for every 1 second period and at the end of the transfer period it computes and reports the average goodput experienced for the entire connection. The offloading procedures are performed twenty times and the average packet loss ratio and goodput computed. During the test procedure for the IP flow mobility functionality, only the file transfer service is offloaded to the WLAN access.

It is expected that the time at which the offloading event is triggered would affect the average packet loss ratio experienced by the video stream in both the scenarios. In the first scenario, after moving both IP flows to the WLAN access the video stream could experience little to no packet loss, since the WLAN access is not congested and has the available resources to accommodate both the traffic flows. In the second scenario, when moving the TCP flow to WLAN more resources are available for the video stream (the network becomes less congested) and thus experiences little to no packet loss. Hence, it is expected that the earlier the offloading event is performed the less packets will be lost. A similar analogy is expected for the average goodput experienced by the file transfer. This is because according to the testbed configurations the WLAN access network has more capacity to offer the TCP stream (file transfer) than the LTE access, and the access is not congested. The TCP stream can thus achieve a much greater transmission rate in the WLAN access than the LTE access. Hence, it is expected that the earlier offloading is triggered, the greater the average goodput of the file transfer.

5.1.4.2 Results and analysis

Figure 5.2 illustrate the average packet loss ratio in percentage experienced by the video stream for different offloading times for the two scenarios. The recommended packet loss ratio requirement of 1% for IPTV service is also shown in the figure. The results are

measured from a sample of 6859 packets captured for a period of 200 seconds at the MDF and the UE, and the offloading event is triggered in increments of 40 seconds until 200 seconds.

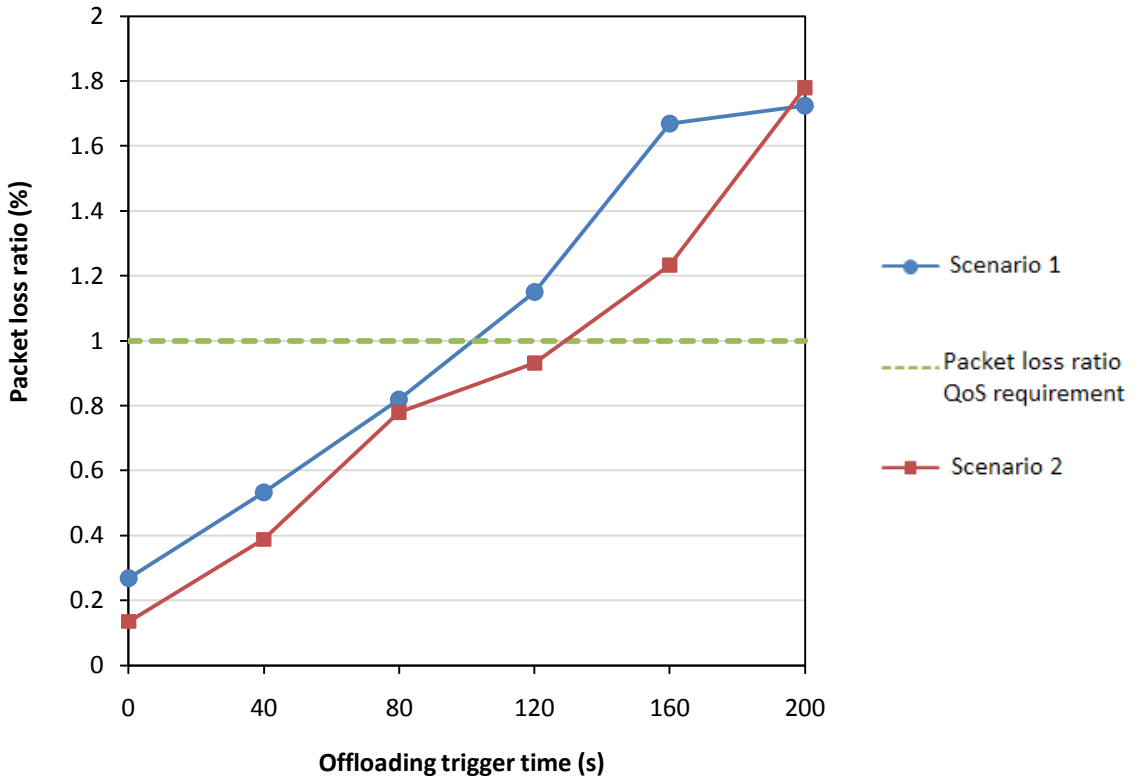

Figure 5.2: Comparison of the packet loss ratio of the IPTV service for the two WLAN offloading functionalities and the packet loss ratio requirement for different offloading trigger times

It is observed from the results that the packet loss ratio increases as the offloading trigger time increases. This result confirms the expected trend of packet loss ratio against offloading trigger time as mentioned previously. It is also observed that the first scenario produces slightly more packet loss than the second scenario. It is expected that the lost packets are incurred due to the handoff of the video stream, since during handover the transmission rate of the video streams stays constant, which means that the MDF continues sending packets to the UE even if the attachment to the WLAN access network has not been completed. Packets sent during this period (handover period) are lost. With the testbed configurations used in the test, it was noticed that before the offloading event the video stream experiences similar packet loss ratios with both scenarios, since the testbed and traffic configuration are similar for each case in the LTE access (observed from the offloading trigger time of 200s, i.e., not offloading to WLAN). It is expected that the packet loss before the WLAN offloading are

occurred at the eNodeB, since even though the PCC in the testbed reserves resources in the core network (S-GW, ePDG and PDN-GW) the eNodeB emulation has no QoS mechanisms i.e., resource scheduling, bearer management [11], queuing methods on the physical interfaces of the machine, etc. Thus, all the packets (video, voice and data packets) at the eNodeB are treated the same e.g., if a voice packet arrives at the eNodeB and the queue on the interface is full, the voice would be dropped (a QoS mechanism would ensure that the voice packets are treated with a much higher priority than data packets [11]).

Comparing the results of the two scenarios to the recommended packet loss ratio, it is observed that in both, offloading the video service to WLAN meets the recommended requirement, but only until a certain period of time during the communication: In the first scenario the end-users would perceive video quality degradation when offloading from 100 seconds onwards during the communication, and with the second scenario the end-user would perceive video quality degradation when offloading from 130 seconds onwards during the communication.

Figure 5.3 illustrates the average goodput for the file transfer service obtained from the two scenarios for varying offloading trigger times.

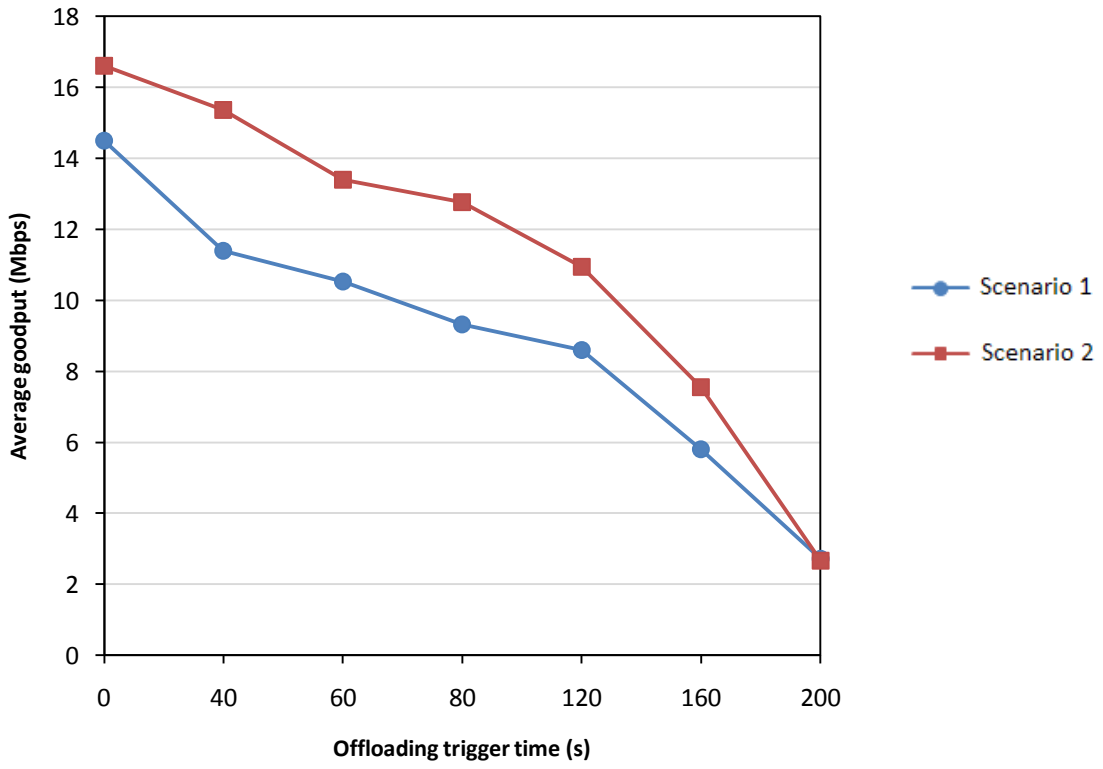

Figure 5.3: Comparison of average file transfer goodput experienced with the two WLAN offloading functionalities for different offloading trigger times

The maximum and minimum average goodput the file transfer could achieve in the first scenario is 14.5 Mbps and 2.7 Mbps respectively, and in the second scenario the maximum and minimum average goodput is 16.6 Mbps and 2.6 Mbps respectively. The results show that, as expected, the goodput both scenarios decreases as the offloading trigger time increases. The reasoning behind this trend is as explained previously.

It is also observed that on average, the file transfer service achieves a larger goodput in the second scenario than in the first; the results are as expected. The reason for the higher goodput is that in the first scenario both the video streaming and file transfer services are offloaded to the WLAN access, and though the WLAN access can support both services (as it is not congested), the available capacity would be shared amongst the two services. The reason being that the IPTV service is based on UDP and according to the basic operation of the UDP, the protocol would transmit packets at a constant transmission rate (unless its variable bit-rate service), whereas with TCP, the transmission rate of the connection would continually be adjusted as TCP incorporates flow control (sender/receiver speed matching) and congestion control (to ensure that the sender throttles its transmission rate when the network gets congested) mechanisms [56] that when triggered would result in either an increase or decrease of the transmission rate of the connection (more on TCP flow-control and congestion control can be found in [56]). Since the UDP service use a portion of the available capacity of the link, the TCP service would use the rest of the available capacity. Many research in the literature exist where the authors evaluate the interaction between UDP and TCP-based services [61] [62] [63], in all the research it has been found that UDP is „unfair" to TCP, since the goodput of TCP-based services reduces in accordance to an increasing UDP bit-rate. Due to offloading only the file transfer service in the IP flow mobility functionality scenario, the TCP connection can take full advantage of the available capacity which means that a greater goodput is obtained at the UE.

The results obtained from this test has shown that for the service combination evaluated, WLAN offloading via IP flow mobility could improve the performance of both the video and file transfer services and could enhance the end-users" experience, and thus proving at least one benefit of the IP flow mobility functionality.

5.2 Evaluation of the proposed IP flow mobility functionality

To evaluate the proposed IP flow mobility functionality, certain metrics are measured that would indicate the effectiveness of the solution. In this section, the effectiveness of the proposed IP flow mobility functionality is assessed based on:

- Whether the designed IP flow mobility functionality would ensure that the disruption experienced by the respective IP flows during offloading are within the 3GPP standardised QoS characteristics of the EPC. A test is performed to measure IP flow handover latency experienced by an IPTV and file transfer service. The effect of all the IP flow mobility enhancements would be evaluated in this test.
- Whether the overheads introduced by the IP flow mobility mechanisms would affect the performance of the machines hosting them and in turn have an effect on the end-user services and experience. The particular mechanism assessed is the flow-based routing mechanism and the effects it has on the PDN-GW performance, regarding packet processing delay and throughput. Signaling overhead between the EPC entities is also measured, since the proposed solution introduces additional signaling and signaling message data that could have an effect on the overall solution, particularly the session continuity mechanism and the IP flow handover latency. Additional signaling could increase the IP flow handover latency since more signaling requires more processing; this in turn could affect the end-user experience as large latencies could degrade ongoing service quality and could result in service discontinuity.
- Scalability and the ability to handle load. This assessment is done by subjecting the PDN-GW (as it contains the bulk of the proposed enhancements) with multiple simultaneous IP flow mobility requests and measuring the time it takes the PDN-GW to process the requests. The proposed session continuity and IP flow information management enhancements would be evaluated.

5.2.1 IP flow handover latency

IP flow handover latency is defined as the period of time the UE experiences a disruption in its packet stream during an IP flow handover. 3GPP defined QoS characteristics that need to be met within the EPC in order to meet the QoS requirements [11] of certain services; one particular QoS characteristic that applies to the IP flow handover latency is the packet delay

budget. Packet delay budget is the maximum acceptable end-to-end delay that a packet of a particular service should experience when sent from the PDN-GW to the UE, and vice versa. For IPTV, 3GPP recommended a maximum packet delay budget of 300 ms and for file transfers, email and peer-to-peer (p2p) services they recommend 300 ms [11]. The IP flow handover latency should be within the recommended packet delay budget in order to ensure an acceptable quality of the service. Handover latencies could have varying affects on the end-users experience. For instance, if an end-user is performing a file transfer that is scheduled to complete in 10 minutes, an additional 500 ms would not be perceivable to the end-user. However, for a real-time video service large handover latencies tend to result in more packet loss (i.e. with real-time services any packets that are not received within a given time frame are unusable and considered lost) that could result in unnatural pauses in the audio/video play-out and image distortion that is perceptible to the end-user.

The IP flow handover latencies experienced by the IPTV and file transfer service are measured and the results compared to the recommended maximum packet delay budget of the services in the EPC. The IP flow handover latency is measured for the scenario when the IP flow is moved to the WLAN access network and the LTE access network. The same testbed configuration as described in section 5.1.1 is used for the measurements. The handover latency is computed as the difference in the time from when the IP flow handoff trigger is sent to the network until the time the first downlink packet of the IP flow arrives on the new interface. The Wireshark protocol analyser tool is used to record the respective times. The handover procedures are performed fifty times and the average recorded.

Figure 5.4 illustrates a comparison of the average IP flow handover latency measured for the individual IP flows during handoff to the WLAN access and LTE access network and the maximum packet delay budget requirement of the services. The average IP flow handover latency experienced by the IPTV IP flow when moved to the WLAN and LTE access networks are 25.3 milliseconds (ms) and 26.1 ms respectively. The average IP flow handover latency experienced by the file transfer IP flow when moved to the WLAN and LTE access networks are 41.4 ms and 48.8 ms respectively.

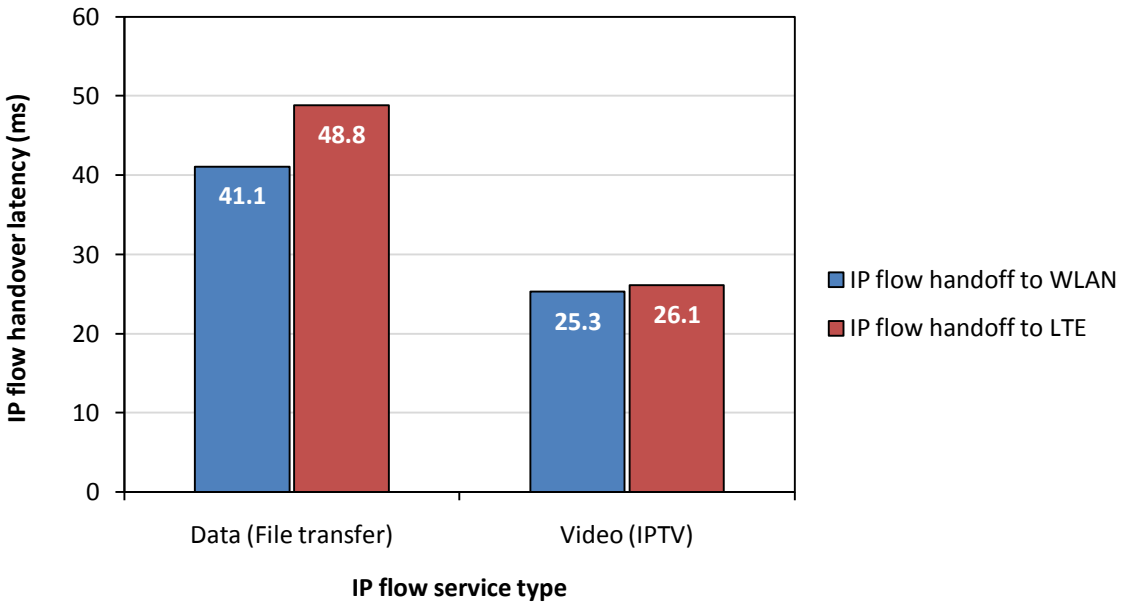

Figure 5.4: Average IP flow handover latencies experienced by the IPTV and file transfer IP flows for handover to LTE and WLAN access networks

The results show that an IP flow handoff with the file transfer service to both access networks results in a larger IP flow handover latency compared to the IP flow handover latency experienced by the IPTV service for the two access networks. The increase is due to the operation of TCP; During the IP flow handover to both access networks, the switch from one access network to the other results in some of the TCP packets not being acknowledged within the currently active timeout interval [56] for the connection. The server responds by momentarily decreasing the congestion window size of the connection and retransmits the already received packets at the UE. The decreased congestion window causes a slight decrease in the transmission rate during offloading. This is unlike the UDP protocol that maintains its transmission rate irrespective of offloading. The UE thus receives the UDP packets faster that the TCP packets after offloading. The results also show that the both services experience slightly larger latency when the offloading is performed to the LTE access network. This is due to the additional processing occurring at the eNodeB emulation node. The user data plane between the eNodeB and the S-GW uses the GPRS tunnelling protocol (GTP-U) [64], meaning that all the packets are encapsulated/de-capsulated between the eNodeB and S-GW and this introduces additional processing. No encapsulation is performed between the UE and the ePDG when offloading to the WLAN access network.

Comparing the IP flow handover latencies of the respective services to the maximum

packet delay budget requirement for the service (i.e., 300 ms requirement for both services), it is observed that an IP flow handoff with both traffic types would not violate the maximum packet delay budget requirement. The low IP flow handover latency is due to the multihoming and session continuity enhancements, enabling the IP flow handovers to be similar to make-before-break type of handovers. Make-before-break functionality means that the UE first establishes connectivity in the target access network before triggering the IP flow handoff to the access. With the IP flow mobility design the UE is connected to the target access network first (i.e., is multihomed) before the IP flow handoff is triggered. Thus, the latencies associated to layer-2 (link-layer) and layer-3 (network-layer) connectivity does not contribute to the total IP flow handover latency.

The IP flow handover latency results measured for the example services have shown that the proposed IP flow mobility functionality introduces minimal disruption during offloading that is within the 3GPP standardised QoS characteristics of the EPC.

In real MNO implementations the IP flow handoff latency would be affected by additional factors like the number of nodes (e.g. routers) in the communication path. More nodes entail more processing and would increase the IP flow handoff latency. Due to limitations of space and due to the nature of the developed testbed, the effect of increasing nodes on IP flow handoff latency are not evaluated and would be considered in future work.

5.2.2 Effect of the flow-based routing mechanism on the PDN-GW performance

The PDN-GW is a high performance entity and any additional overhead could affect its performance. The flow-based routing mechanism imposed on the packet processing logic of the LMA could affect the performance of the PDN-GW, since for every downlink packet addressed to the UE the LMA would have to compare the IP 5-tuple of the packet‟s header to all the routing filters in the UEs flow binding list in order to find the destination (i.e., P-CoA) of the packet. The performance metrics measured are those that could be affected by the mechanism. In particular, the packet processing delay and throughput are measured, since the number of flow binding entries the LMA would have to match for the packet‟s destination could influence both these parameters. For instance, if the flow binding list comprises of 50 entries the LMA would have to match the IP 5-tuple of a single packet to all the routing filters of the 50 entries (for each entry this comprises of matching 5 parameters) and if the routing filter that yields a match is the very last entry in the list, the LMA would have cycled

through 49 entries. There could definitely be a delay incurred in a scenario as described previously which could lead to a decrease in the number of packets that the PDN-GW could transmit within a given interval (i.e., throughput). The goal of the tests performed in this section are thus to quantitatively determine how the throughput of the PDN-GW is affected by the flow-based routing mechanism and delay (if any) this mechanism could impose on a packet.

5.2.2.1 Packet processing delay

Packet processing delay is defined as the time taken to process a packet‟s header and to determine the forwarding path of the packet. Various factors could contribute to the processing delay experienced by the packets in the PDN-GW: a particular factor is the processing capabilities of the PDN-GW machine. The CPU load and the available memory of the machine could affect the overall performance of the machine and thus the processing time. Three PDN-GW load states (CPU and memory utilisation) of 0%, 50% and 90% are thus considered during the measurements. The load in the PDN-GW is introduced with the open source Linux stress [**65**] tool, an overview of the tool is given in Appendix E.1.

5.2.2.1.1 Test procedure

To measure the packet processing delay, two time probes are set in the packet handler source code of the LMA using the *gettimeofday* [66] Linux function. The time probes are placed after step 5 and step 79 as indicated in the pseudo code of the packet handler function in Appendix D.3. The first time probe gives the system time when the LMA starts extracting the IP 5-tuple and the second time probe provides the system time when the LMA has determined the destination to forward the packet to. The difference in the times recorded is the packet processing delay. The test traffic was generated by establishing a video stream from the MDF. The video stream has a constant bit-rate of 600kbps and the packets have varying sizes ranging between 840 to 1400 bytes. Packet processing delay is not affected by packet size nor bit rate [67] since only the header of the incoming packets are inspected and the same packet processing procedure is performed irrespective of when the packet arrives. The only additional factor that could influence the delay is the size of the flow binding list.

For each packet, the processing delay is calculated (during the processing procedure) and stored to a text file. The average packet processing delay of 1500 samples are then computed. The packet processing delay is measured and compared for two scenarios: The first scenario

considers a PDN-GW without a flow binding list of entries and the second scenario considers the PDN-GW with a flow-binding list of entries. The two scenarios for the test procedures are illustrated in figure 5.5. Comparing the two scenarios would indicate the delay expected with the implementation of the IP flow mobility solution and would allow an analysis on whether the delay could be considered negligible or whether a substantial delay would be introduced and thus rendering the functionality impractical.

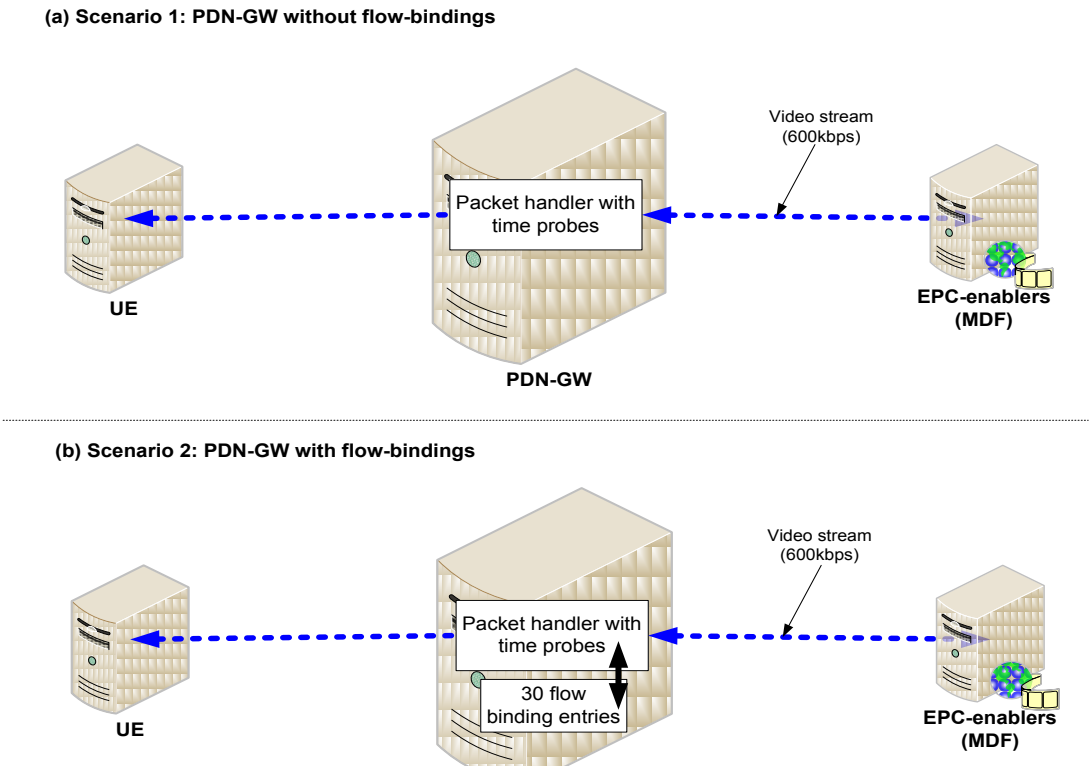

Figure 5.5: Scenarios setup for measuring the PDN-GW packet processing delay

In the second scenario, the number of flow bindings is set to a constant value of 30. This value is based on the assumption that the UE could have a maximum of 30 IP flows running at any given time. The first 29 entries contains routing filters that will ensure that the PDN-GW match all the received packets to the filters, but will not permit the PDN-GW to forward the frames to the ePDG. All the 29 routing filters have the same transport protocol (i.e., UDP), source and destination IP address (i.e., IP address of enablers and IP address of the UE interface) and the source port (i.e., port used by the Iperf server) parameters, the only difference in the filters is the destination port number. The destination port number is the last parameter compared during the routing filter matching procedure. With this setup, the PDN-GW will have to match a maximum of four entries for each routing filter during the search.

The last entry (i.e., the 30th) contains the routing filter that contains the conditions that will permit the PDN-GW to forward the received packets to the ePDG machine.

5.2.2.1.2 Results and analysis

Figure 5.6 illustrates the comparison of the average packet processing delay for the two scenarios. The y-axis represents the packet processing delay in microseconds (µs) and the x-axis represents the different PDN-GW loads in percentage.

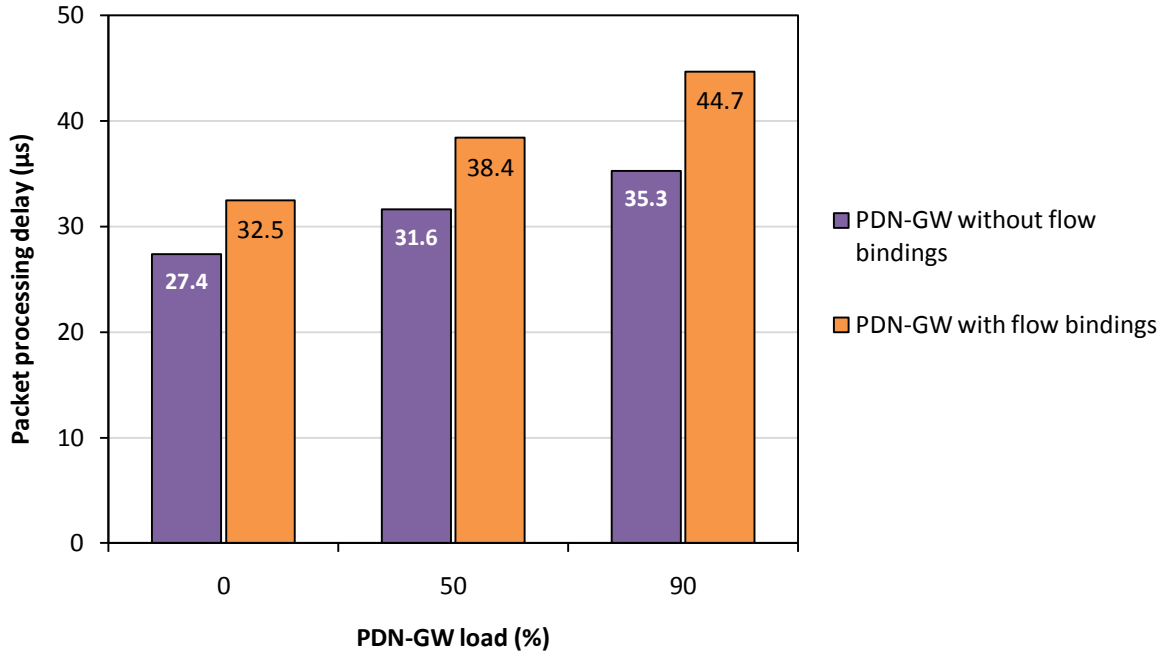

Figure 5.6: Average packet processing delay comparison for a PDN-GW with and without a flow-binding list of entries for different PDN-GW loads

The results show that when the LMA process packets according to the flow-based routing enhancements an additional delay is incurred during packet processing. When the PDN-GW load is 0% the average packet processing delay incurred for the scenario without the flow bindings list is 27.4 µs and for the scenario with the flow binding list the average packet processing delay is 32.5 µs. The packet processing delay thus increases by 5.1 µs when the flow bindings are considered during packet processing. Similarly, for a PDN-GW load of 50% and 90% the average packet processing delay for the scenario without the flow bindings is 31.6 µs and 36.3 µs respectively and for the scenario with the flow binding list the average packet processing delay is 38.4 µs and 44.7 µs respectively. The packet processing delay thus increases by 6.8 µs and 8.4 µs when the flow bindings are considered during packet

processing for a PDN-GW load of 50% and 90 % respectively. As expected, the packet processing delay also increases as the PDN-GW load increases, since the LMA cannot process the packets with all the available resources (CPU, memory, etc) in the PDN-GW.

Evaluating the packet processing delay results and considering that the test concerned a single flow binding list and UE, the packet processing delay could be considered as negligible. This observation is true even in a scenario where 1000 UEs each have a flow binding list of 30 entries. In this scenario, any packet addressed to a particular UE would only be delayed (i.e., packet processing delay) for a period of time it takes the LMA to process the packet according to that UEs flow binding list, and not a list comprising of all the 1000 UEs flow bindings. The affect of the flow-based routing mechanism on packet processing delay is thus insignificant.

5.2.2.2 Throughput

Throughput is the defined as the total number of bits the PDN-GW could transmit on its outgoing interfaces within a time period of 1 second. The measurement unit used for throughput is bits per second (bps). The throughput measured is the interface to interface throughput of the PDN-GW. The PDN-GW of the testbed has three interfaces: the SGi interface (towards the Enablers machine) and the S2b and S5 interfaces (towards ePDG and S-GW machines respectively). All the interfaces are capable of transmitting at speeds of 100Mbps; the SGi and S2b interface of the PDN-GW is used for the throughput measurement.

5.2.2.2.1 Test procedure

The test procedure is performed for the same two scenarios as for the packet processing delay, and is illustrated in figure 5.7. The flow binding entries setup in the second scenario is the same as with the packet processing delay test.

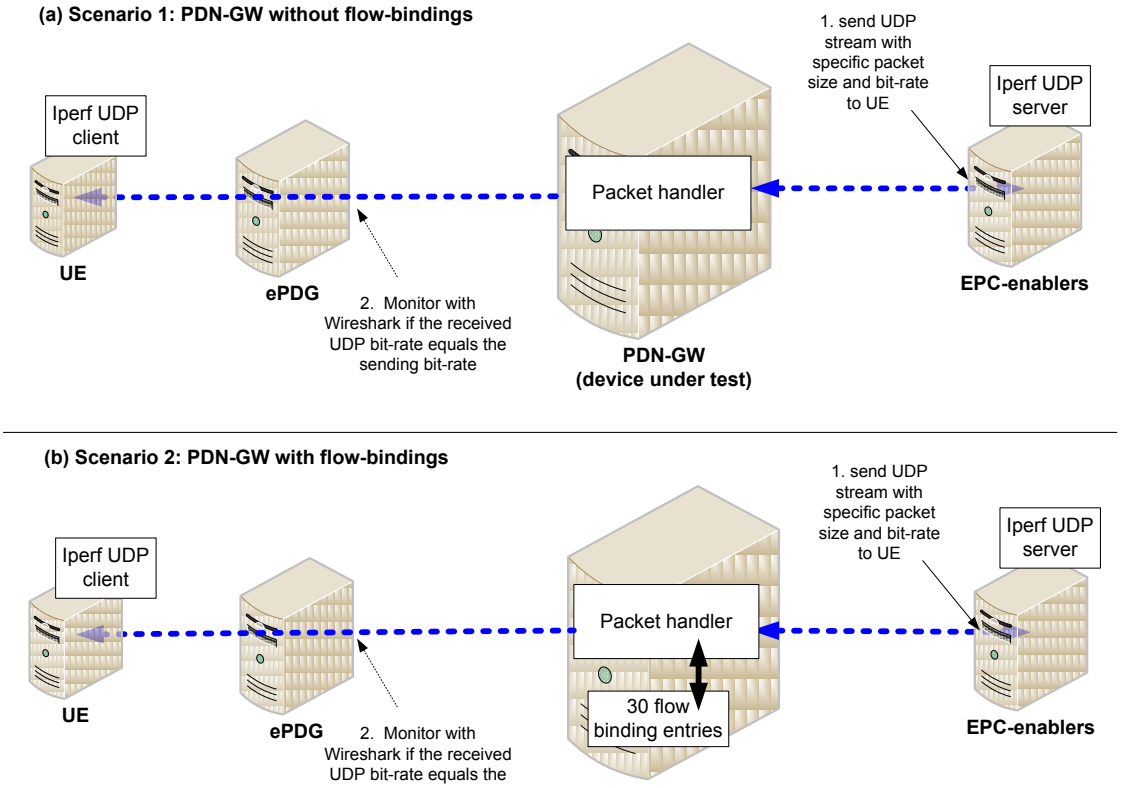

Figure 5.7: Scenarios setup for measuring the PDN-GW throughput

The test procedure for measuring the throughput is as follows: Using Iperf, with the Iperf server in the Enablers machine and the Iperf client in the UE machine, a UDP stream with a specific packet size and rate is sent to the PDN-GW machine. The number of packets sent to the PDN-GW is counted by the Iperf server, and the number of packets received is counted at the ePDG interface with the Wireshark analyser tool. If the number of packets received (by the ePDG) is equal to the number of packets sent to the PDN-GW, the throughput is the rate of the test stream. If fewer packets are received than were transmitted by the Iperf server, the rate of the stream is reduced and the test rerun. The throughput is measured as the fastest rate at which the count of test packets transmitted by the PDN-GW is equal to the number of test packets sent to it from the Iperf server. The packet sizes (in bytes) used for the test stream are: 64, 128, 256, 512, 1024, 1280 and 1420. These packet sizes are chosen as it would provide a full characterisation of the throughput of the PDN-GW for common packet sizes that could be transmitted in the network [68] [69] and since it would not violate the maximum and minimum frame sizes permitted by the Ethernet standard [70] [71]. Ethernet is used between the testbed entities; the maximum transfer unit allowed is 1500 bytes and the minimum is 64 bytes [68] [71]. Packets that would result in a frame size of more than 1500

bytes would result in fragmentation i.e., packets would need to be divided into pieces at the PDN-GW (the outgoing interface) in order to transmit the packet over the link to the ePDG. This usually entails more processing and could affect the results measured [71].

5.2.2.2.2 Results and analysis

Figure 5.8 illustrates the throughput measured for the two scenarios for the different packet sizes. The x-axis indicates the different packet sizes in bytes and the y-axis indicates the maximum throughput in Mega bits per second (Mbps) for the different packet sizes.

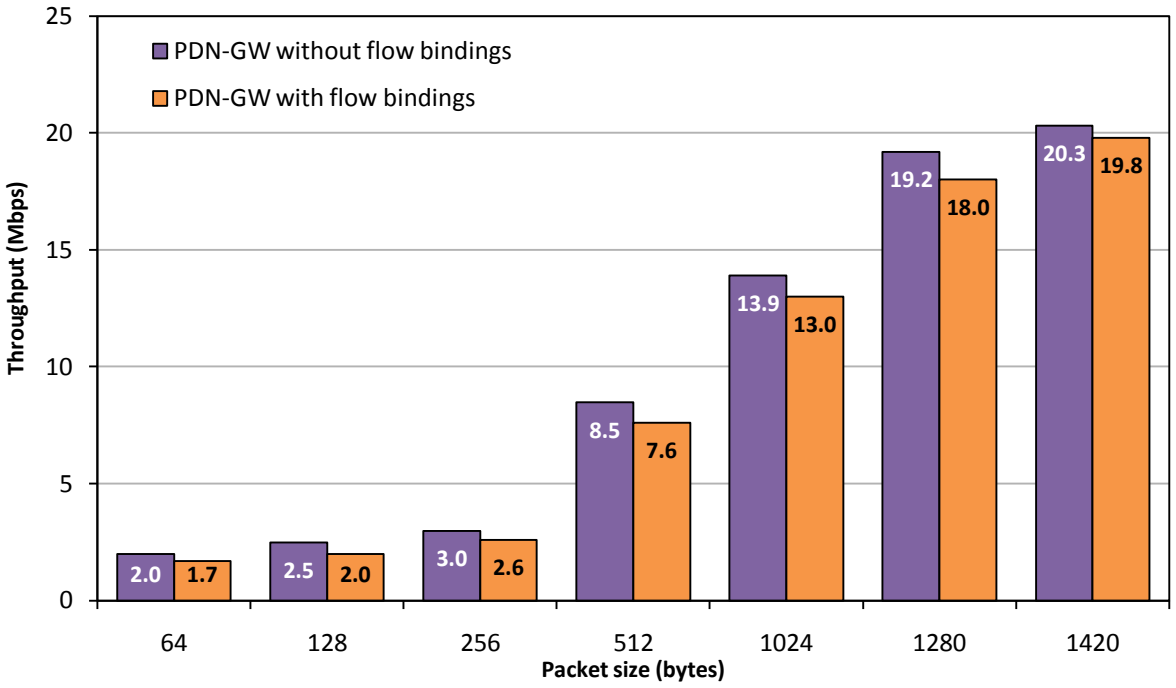

Figure 5.8: Comparison of the throughput measured for different packet sizes for a PDN-GW with a flow binding list and a PDN-GW without flow binding list

The minimum and maximum throughput measured for the PDN-GW without the flow bindings table is 2 Mbps and 20.3 Mbps respectively. The minimum and maximum throughput measured for the PDN-GW with the flow bindings table is 1.7 Mbps and 19.7 Mbps respectively. The results indicate that the throughput for both the scenarios increases as the packet size increases. The lower throughput experienced with small packet sizes is due to smaller packets demanding more frequent forwarding decisions that for larger packets within the same time period e.g., the processing delay incurred by 100 64-byte packets could be equivalent to processing 10 512-bytes packets, hence for smaller packets fewer packets are transmitted within a period on the outgoing interface.

Comparing the throughput of the PDN-GW with the flow-binding list against the throughput of the PDN-GW without the flow-binding list, it is observed that for all packet sizes the throughput of the PDN-GW with the flow binding list enabled is slightly less than the PDN-GW without the flow-binding list. The reduction in the throughput is expected since the PDN-GW with the flow-binding list of entries would have to perform additional processing of the packets (irrespective of the packet size) which means that packets remain longer within the PDN-GW, resulting in less packets being forwarded/switch between the input and output interface.

The throughput measured is representative of only a UE with a single flow binding list. It is expected that with an increase in the number of flow binding lists and with a vast amount of different IP flows the PDN-GW would have to match for many UEs, the throughput of the PDN-GW would significantly reduce since the amount of processing the PDN-GW would have to perform would automatically increase. So unlike the packet processing delay measured previously that is independent of the number of flow binding lists the PDN-GW would have to process, the throughput of the PDN-GW is not independent of the number of flow binding lists. With this conclusion, there is certainly a need for future optimisations to the proposed mechanism since throughput is one of the major performance indicators of network entities.

5.2.3 Load testing

The PDN-GW is a high capacity core network entity that would be required to serve multiple IP flow mobility requests from a large subscriber base in commercial implementations. In this section the processing delay of the PDN-GW is analysed when it is subjected to multiple simultaneous IP flow mobility requests.

The time taken to process a PBU message with a routing rule mobility option, process the information in the routing rule mobility option, create a flow binding in the flow binding list, search for additional routes belonging to the end-user and create the PBU message with the end-users additional route, is measured. This operation encompasses the entire overhead introduced by the proposed session continuity and the IP flow information management extensions. This operation could have an overall effect on the entire system, it is thus imperative to investigate the effects different loads of IP flow mobility requests might have on the execution.

To measure the effect of increased IP flow mobility requests, tests are performed to

measure the processing delay incurred at the PDN-GW when the number of IP flow mobility requests are increased from 1 to 100. The IP flow mobility requests are sent to the PDN-GW with constant inter-arrival times from the ePDG. The processing delay is measured as the time from receiving the first PBU message with routing rule mobility option from the ePDG to the time a PBA message is sent back to the ePDG for each individual IP flow mobility request. The processing delay is measured with the Wireshark network analyser tool on the S2b interface of the PDN-GW. Figure 5.9 illustrates the measured processing delay at the PDN-GW as a function of the number of IP flow mobility requests.

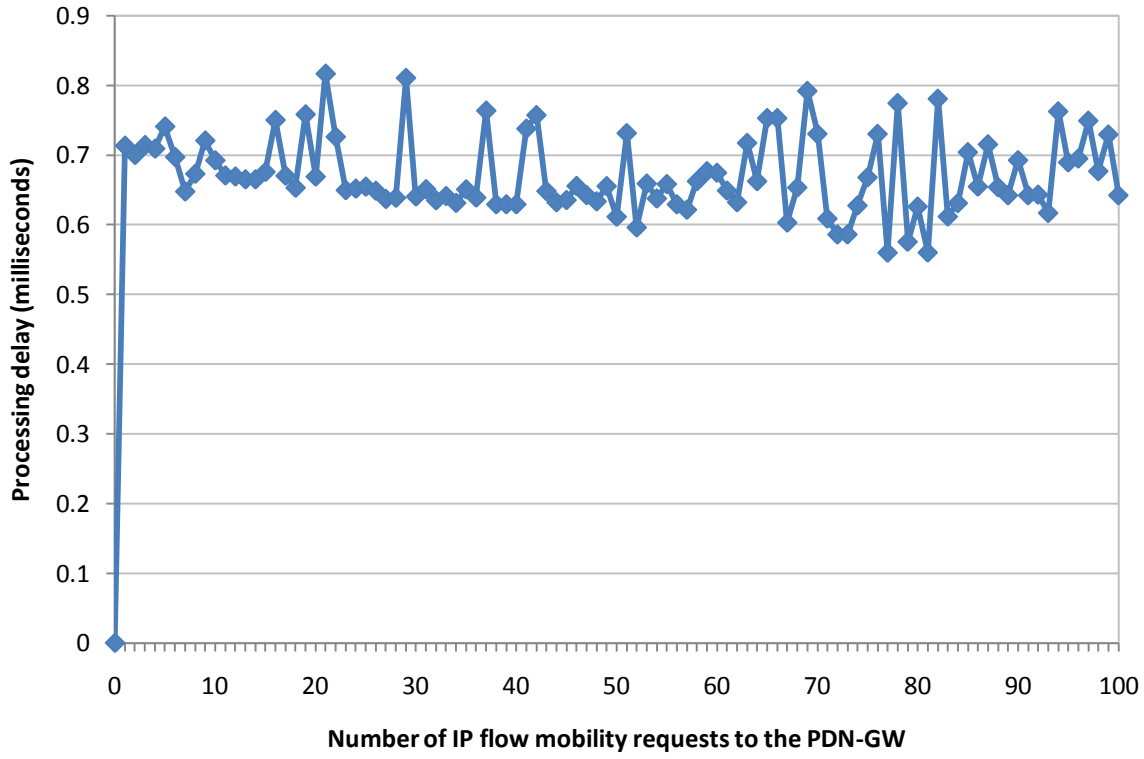

Figure 5.9: Processing delay of PDN-GW as IP flow mobility requests increases

The results show that as the number of IP flow mobility requests increases the average processing delay of the PDN-GW fluctuates on average above 0.6 milliseconds and ranges between 0.5 – 0.84 milliseconds on some IP flow mobility requests. The recommended signaling message processing delay for the PDN-GW according to 3GPP is 5ms [10]. The results obtained shows that the PDN-GW with the IP flow mobility enhancements still performs within the acceptable recommendation.

The results also indicate that the processing delay of the PDN-GW stays unaffected as the number of IP flow mobility requests increases. However, in commercial implementations

the results may vary, since the test considers scalability only to a limited extent. The performance of the PDN-GW in the testbed implementation is dependant on the host machine‟s hardware specification and the operating system. PDN-GWs in commercial implementations would have different hardware specifications.

Further testing was also conducted to determine the performance of the PDN-GW when the number of IP flow mobility requests increases beyond 100 IP flow mobility requests per second. From the results obtained, it was observed that beyond 100 IP flow mobility requests per second, the processing delay of the messages increases exponentially. For 120 IP flow mobility requests per second, the processing delay was found to be 78.9 milliseconds on average, and for 140 IP flow mobility requests per second, the processing delay was 262.2 milliseconds on average. The rapid increase in processing delay is due to queuing occurring within the PDN-GW. The requests are queued in a first-in-first-out manner, meaning that the additional processing delay is due to the time it takes the PDN-GW to process the requests. The more requests are queued the longer the delay.

5.2.4 Signaling overhead

The signaling overhead is defined as the total additional mobility signaling messages or message data in bytes sent between the EPC network entities to achieve an IP flow handover. To measure the signaling overhead, there needs to be a base signaling methodology to compare with the signaling methodology of the IP flow mobility functionality. The base signaling methodology used is the standard PMIPv6 vertical handoff, as this provides an indication of the expected overhead introduced when IP flow mobility functionality is deployed within the network. The high level overview of the signaling methodology of the standard PMIPv6 vertical handoff from LTE to WLAN is discussed in Appendix E.2 and in chapter 8 of the 3GPP standard [4]. The IP flow mobility functionality signaling methodology is also discussed in Appendix E.2.

The signaling messages generated between the machines hosting the EPC network nodes are captured and measured by monitoring all the interfaces using the Wireshark protocol analyser tool. The measurements are carried out only once since the signaling messages are constant during each scenario. The results obtained for the two scenarios are shown in Table 5.1. The first row in the table provides the results of the total signaling load in bytes for the two scenarios and the second row provides the results for the signaling overhead in percentage incurred by the IP flow handoff scenario.

Table 5.1: Signaling load and overhead incurred by each scenario for handover to WLAN

	PMIPv6 vertical handover	IP flow handoff
Signaling load (bytes)	13668	13984
Signaling overhead (%)	-	2.3%

The total signaling load when a handover is performed with PMIPv6 is 13668 bytes. The total signaling load for the IP flow handoff 13984 bytes. The signaling overhead thus increases by 2.3% for the IP flow handoff scenario. This overhead is due to an additional PBU and PBA message sent for the IP flow handoff procedure. The PBU contains the routing rule mobility option data (Appendix A.4) and the PBA contains the end-user‟s previously assigned HoA/HNPs in the additional route mobility option (Appendix A.3).

The signaling overhead measured is for a single IP flow handover of a single UE. In a scenario where multiple UEs each perform an IP flow handoff the signaling in the core increases by a factor equivalent to the number of UEs. Thus, for 100 UEs performing an IP flow handoff, 200 mobility messages, equating to an additional 31600 bytes (i.e., 31.6kB) will traverse the core network (between the ePDG and PDN-GW). The signaling overhead introduced by the IP flow handoff could be considered as insignificant since though the evaluation framework comprises of high performance desktop machines, the real EPC network elements have much greater performance capabilities and would be interconnected with higher performance links, a mere 316 bytes of additional signaling would not overload the core entities.

5.3 Discussion

This chapter has presented an evaluation of the proposed IP flow mobility functionality presented in the previous chapters. Proof of concept tests were performed to validate the IP flow mobility mechanisms and show that IP flow mobility could enhance application performance and improve end-user experience. The results of the proof of concept tests has shown the effectiveness of the designed IP flow mobility functionality in responding to requests from the end-user regarding the preferred access network for an IP flow and redirecting an IP flow without session discontinuity between the access networks. It was also shown that IP flow mobility could enhance the application performance and could enhance end-users experience.

The evaluation of the proposed IP flow mobility functionality was performed by measuring the IP flow mobility handoff latency to determine whether it is within the 3GPP requirements for the EPC. The result from the test has shown that the IP flow handover latency meets the requirement by 3GPP. The overheads introduced by the IP flow mobility enhancements were also measured to determine the effect it could have on network performance and consequently end-user experience. The results from these tests have shown that there are overheads introduced by the IP flow mobility functionality i.e., increase in packet processing delay and a reduction in throughput of the PDN-GW, as well as signaling overhead between the EPC network entities, but these overheads do not significantly affect the network performance. These overheads are expected from functionality like IP flow mobility, since it involves additional mobility signalling and imposes packet classification requirements to the PDN-GW of the EPC. A test was also performed in order to evaluate how the solution handles load i.e., multiple simultaneous IP flow handoff requests; the processing delay of the PDN-GW was measured in this test. The result showed that as the number of IP flow handoff requests increase the processing delay is unaffected.

Based on the analysis of the results it is concluded that the proposed IP flow mobility functionality adheres to the design considerations outlined in chapter 3. The next chapter concludes the dissertation and proposes recommendations for future work within the IP flow mobility area.

Chapter 6

Conclusions and future work

6.1 Conclusions

The focus of the research conducted throughout this dissertation is on the design, implementation and analysis of PMIPv6-based IP flow mobility functionality for 3GPPs EPC. IP flow mobility functionality is a technique that would enable Mobile Network Operators (MNOs) to intelligently offload mobile data traffic from congested macro access networks like 3G and LTE to complementary access networks like WLAN in order alleviate congestion in the macro access networks and to increase network capacity. The need for IP flow mobility functionality arose since the conventional WLAN offloading functionalities only enables MNOs to offload the entire end-users traffic to WLAN and in the process degrading the end-users ongoing services, whereas IP flow mobility functionality would enable MNOs to augment the end-users quality of experience of services as it enables offloading only a subset of the end-users traffic to WLAN (e.g. non-real time file transfer services with less stringent QoS requirements) while at the same time leaving the rest of the traffic on the macro access networks (e.g. real-time services with stringent QoS requirements).

A literature review was conducted to identify the functional requirements for designing IP flow mobility functionality for 3GPPs EPC, and to determine the functionality missing from the PMIPv6 mobility solution of the EPC, the related works and the current PMIPv6 IP flow mobility proposals by the 3GPP and IETF standardisation bodies. It was found that from

a mobility management perspective, IP flow mobility schemes require key components that include a mechanism to ensure session continuity during IP flow handoff and a mechanism that would enable flow-based routing and IP flow information management, and that the PMIPv6 mobility solution of the EPC lacks these mechanisms. The related works in literature on PMIPv6-based IP flow mobility functionality are also not based on 3GPPs PMIPv6 mobility solution for the EPC and none of the works evaluate the performance of their schemes or developed a prototype of their schemes on an EPC testbed. Thus the goal of this work is to propose enhancements, based on the works in the literature, to the 3GPP PMIPv6 mobility solution to enable both the mechanisms required for IP flow mobility functionality and evaluate the proposed functionality on an EPC testbed.

To address the session continuity challenge PMIPv6 faces with IP flow mobility, this dissertation proposes enhancements to the functional procedures of the PMIPv6 protocol. These enhancements enable the PDN-GW/LMA functionality to send all the home network prefixes of a specific UE to the access gateways (that hosts the MAG functionalities of PMIPv6) and enabling these gateways to forward any traffic belonging to the end-user. To complement the proposed session continuity enhancements, the design requires the end-user devices to support and implement the weak-host model. The proposed enhancements conform to the 3GPP and IETF standards and do not increase the UE complexity. To address the flow-based routing and IP flow information management challenge with PMIPv6, this dissertation proposes further enhancements to the functional procedures of PMIPv6. The proposed enhancements are based on concepts adapted from the IETF standardisation body. The proposed enhancements introduce the concept of flow-bindings, enabling the PDN-GW/LMA to identify and route traffic based on IP flow descriptors and preferences from the end-user. The end-user can establish a list containing the information of all the current IP flows in the PDN-GW/LMA and indicate to the PDN-GW/LMA the preferred access network for each of the IP flows.

A prototype of the proposed IP flow mobility functionality was developed on an emulated EPC testbed using the OpenEPC software toolkit developed by Fraunhofer FOKUS. The software toolkit has all the requirements for emulating the complete EPC entities and provides a standards compliant implementation of the PMIPv6 mobility protocol. The PMIPv6 mobility enablers of the OpenEPC toolkit were enhanced with the proposed mechanisms to realise the IP flow mobility functionality. The testbed was then used to show proof of concept and to evaluate the IP flow mobility functionality.

Based on the results and findings of this dissertation, the following conclusions are

drawn:

- Proxy Mobile IPv6 supports multiple interfaced UEs to simultaneously attach to different access networks in the EPC, but experiences difficulty in managing these multiple interfaces in order to support session continuity during handovers between the attached interfaces. Session continuity is a requirement of any mobility solution and multihoming is a requirement for IP flow mobility. Thus, a multiple interface management scheme is necessary for the Proxy Mobile IPv6 technology in order to fulfil the requirements of mobility solutions and IP flow mobility. The session continuity mechanism proposed within this dissertation can successfully achieve the latter requirements.

- The IP flow mobility functionality with Proxy Mobile IPv6 is dependent on procedures for controlling the changing of the IP flows to different accesses. The complexity for enabling this mechanism was evident in this work, since it had required enhancements to the protocol procedures, signaling messages and packet forwarding procedures in the PDN-GW. However, the benefits that the base IP flow mobility functionality could offer to MNOs and end-users far outweighs the complexity necessary for the scheme. From the findings of the tests it was observed that the IP flow mobility functionality imposes additional overhead (i.e., increases packet processing delay of the PDN-GW, incurs signaling overhead in the core network and reduces the throughput of the PDN-GW) in the EPC network, but some of these overheads (packet processing delay and signalling overhead) are considered negligible while the throughput degradation incurred by the PDN-GW needs to be addressed.

- The results have shown that the IP flow mobility functionality is feasible for moving TCP and UDP based IP flows between the LTE and the WLAN access. However, to effectively move a TCP based service between the access networks and consequently the UEs interfaces, the UE needs to be aware of the movement in order to reflect the path for sending the TCP acknowledgements to the TCP sender.

- Comparing the video and file transfer performance for the WLAN offloading scenario with the IP flow mobility functionality against a WLAN offloading scenario without IP flow mobility functionality, it was shown that IP flow mobility functionality improves the performance of the applications and could thus enhance the end-users experience. This supports one of the benefits of why IP flow mobility

functionality should be incorporated and considered for WLAN offloading in the EPS.

- The EPC is characterised for providing seamless handovers to mobility devices. It was observed that handovers with the IP flow mobility functionality conform to the packet delay budget thresholds of the real-time and non-real-time services in the EPC. Thus, it is concluded that the proposed IP flow mobility functionality adhere to the performance characteristics of the EPC.
- The proposed IP flow mobility functionality enhancements in the PDN-GW is subject to multiple simultaneous IP flow mobility requests ranging from 1 to 100. This evaluation assesses the ability of the PDN-GW to handle load and the viability of the proposed enhancements when processing multiple requests simultaneously. The results obtained from the evaluations show that the IP flow mobility enhancements in the PDN-GW imposes a negligible effect on the message processing delay for requests until 100. The average message processing delay was found to be 0.8 milliseconds, which conforms to the requirements of the 3GPP of 5 milliseconds. However, the testbed is not a commercial implementation, it comprises of standard Personal Computer (PC) hardware which means that the results obtained are those that reflect how the implemented system (i.e., PDN-GW) performs with the hardware specification of the PC. Beyond 100 IP flow mobility requests per second, the message processing delay increases exponentially, since the requests are queued by the PDN-GW in a first-in-first-out manner. The queuing adds significant delay equivalent to the period it takes the PDN-GW to process the request.

6.2 Future Work

While conducting this work, a number of key issues were encountered during the implementation of the work and identified within the literature. These issues are not directly addressed in this dissertation, but could be used as a basis for future work.

- The proposed IP flow mobility functionality relies heavily on the principle that MNOs deploy the EPC network using Proxy Mobile IPv6 as the network-based mobility solution. The EPC network also supports the GPRS Tunneling Protocol (GTP) as network-based mobility solution, and since GTP is the primary mobility solution in 2G and 3G architectures, MNOs could deploy the GTP protocol for mobility as it

would provide for easy integration with their existing mobile architectures. Future work could investigate how to adapt the mechanisms of the proposed IP flow mobility functionality or develop new IP flow mobility mechanisms for GTP-based EPC architectures. 3GPP has started investigating this possibility in a release 12 technical report [26] on network-based IP flow mobility support in the EPC.

- The Proxy Mobile IPv6 mobility solution is only effective for providing mobility between MAGs belonging to the same LMA. The PMIPv6 standard does not recommend how mobility (while maintaining session continuity) can be performed between MAGs belonging to different LMAs (PDN-GWs). There have been work done in the literature to solve this issue [72] [73]. The proposed IP flow mobility functionality also have this limitation since all the mechanisms for the managing and routing of IP flows reside in a single PDN-GW with no provision for relocating an IP flow to a different PDN-GW situated in a different domain. Future work could investigate a scenario where the WLAN and LTE access gateways are serviced by different independent PDN-GWs and how an IP flow could be offloaded from the LTE to the WLAN access in such a scenario.
- The proposed flow-based routing mechanism requires the PDN-GW to perform some form of packet identification and classification which does affect the performance of the PDN-GW i.e., increases packet processing delay and reduces the throughput. Future work could consider optimising the mechanism to limit the performance defects on the PDN-GW. An optimisation could be to classify and mark packets before it reaches the PDN-GW. This could reduce the processing required by the PDN-GW since it would then identify only the packets with the specific mark (and not with the complete IP 5-tuple) and forward them to their destination.
- Lately there have been much research regarding the Proxy Mobile IPv6 protocol and its drawback of being a centralised mobility solution, meaning that there is a central entity (the LMA/PDN-GW) through which all the end-users traffic should be routed. The drawback of this is that the PDN-GW becomes a central point of failure and a possibility of becoming a bottleneck entity. Distributed mobility managements solutions [74] [75] [76] are being investigated as possible solution for overcoming this drawback. Distributed mobility management entails redistributing the functionality of the LMA e.g., moving the routing functionality (i.e., tunneling) to the access gateways while leaving the control functionality (e.g., address assignment) in the PDN-GW,

such that there is no central entity performing all the tasks of the PDN-GW. The IP flow mobility functionality is a centralised solution since all the control and routing mechanisms are located within the same entity (i.e., the PDN-GW). Future work could investigate the possibility of designing an IP flow mobility scheme where the underlying PMIPv6 mobility solution is a distributed mobility solution in the EPC.

- IP flow mobility functionality has many benefits as explained in chapter 1 of this dissertation. However, due to the scope, only one of the benefits of IP flow mobility have been investigated in this work i.e., the benefit of enhancing end-user QoE. Future work could investigate using the proposed IP flow mobility functionality and designing intelligence to showcase bandwidth aggregation [77] [78] and load balancing schemes [79] [80] for the EPC. For the bandwidth aggregation scheme there would need to be a packet scheduler that would split and transmit the packets across different links. The scheduler could be in the PDN-GW and interfaced with the routing module. At the UE there would need to be a packet reordering algorithm to reorder the received packets into the correct sequence as it arrives. If TCP IP flows are used, consideration needs to be made for how the TCP acknowledgements will be handled at the UE. For the load balancing scheme, one could consider intelligence in the network that would continually monitor network resources, and trigger the PDN-GW to perform bulk offloading of a particular type of traffic to an access network with more resources. Consideration should be given to determine whether the UEs whose traffic is moved to a different access network is actually attached to that access and how TCP based traffic would be handled.
- The IP flow mobility prototype on the testbed has no intelligence when it comes to the IP flow mobility trigger i.e., why and when the IP flow handoff trigger should be initiated; instead, the IP flow handoff was manually triggered. Future work would investigate this limitation further and would possibly draw on the 3GPP Access Network Discovery and Selection Function (ANDSF) [81] and a network load monitoring tool. The ANDSF is a server capable of sending inter-system mobility policies to the UE through a standardised logical interface (S14 interface). The network load monitoring tool could monitor the load on the LTE access, and if the load reaches a certain threshold it could trigger the ANDSF to send an IP flow mobility policy to the UE, indicating that it should trigger IP flow mobility to the WLAN access.

- Due to the complexity of developing a complete end-to-end IP flow mobility solution that includes resource management on an IP flow level with 3GPPs PCC architecture, charging, resource management and security was not addressed in this work. Future work could investigate the enhancements necessary to PCC architecture for enabling charging control and resource allocation based on IP flows and not complete sessions, and also investigate the security implications, if any, that IP flow mobility might impose or require from the EPC network.

Bibliography

[1] Qualcomm Incorporated. (2010, Mar.) 3G/Wi-Fi Seamless Offload.

[2] 3GPP TS 23.401, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 11)," ver. 11.0.0, Sep. 2012.

[3] 3GPP TS 36.201, "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE physical layer; General description (Release 11)," ver. 11.0.0, Sep. 2012.

[4] 3GPP TS 23.402, "Architecture enhancements for non-3GPP accesses (Release 11)," ver. 11.4.0, Sep. 2012.

[5] WirelessE2E. (2012, May) Analysis of Traffic Offload: WiFi to the Rescue. Whitepaper.

[6] Cisco corp. (2012, Feb.) Cisco Visual Networking Inex:Global Mobile Traffic Forecast Update, 2011-2016.

[7] K. Elleithy and V. Rao, "Femto Cells: Current Status and Future Directions," *International Journal of Next-Generation Networks (IJNGN)*, vol. 3, no. 1, Mar. 2011.

[8] 3GPP TS 23.261, "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload (Release 10)," stage 2, ver. 10.2.0, Sep. 2012.

[9] H. Choi, S. Min, and Y. Han, "PMIPv6-based Flow Mobility Simulation in NS-3," in *Proc. of the 2011 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2011, pp. 475-480.

[10] M. Olsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan, *SAE and the Evolved Packet Core: Driving The Mobile Broadband Revolution*. Burlington, USA: Elsevier, 2009.

[11] 3GPP TS 23.203, "Policy and charging control architecture (Release 11)," ver. 11.1.0, Mar.2011.

[12] L. Yun, Z. Yi-sheng, L. Oi-lie, and W. Feng, "Performance Research of MIPv6 and Extended Protocol in the Process of Handover," in *Proc. of the 5th International Conference on Wireless communications, networking and mobile computing (WiCom '09)*, 2009, pp. 1-4.

[13] M. Masud, F. Anwar, S. Bari, and O. Mohamed, "Enhancement of handoff latency reduction mechanism of mobile internet protocol version 6 (MIPv6)," in *Proc. of International Conference and Communication Engineering (ICCE)*, 2009, pp. 700-705.

[14] K. Kong, W. Lee, Y. Han, M. Shin, and H. You, "Mobility management for all-IP mobile network: mobile IPv6 vs. proxy mobile IPv6," *IEEE Wireless Communications*, vol. 15, no. 2, pp. 36-45, Apr. 2008.

[15] K. Kong, W. Lee, Y. Han, and M. Shin, "Handover Latency Analysis of a Network-Based Localized Mobility Management Protocol," in *Proc. of the IEEE International Conference on Communications (ICC '2008)*, 2008, pp. 5838-5843.

[16] J. Lee, J. Bonnin, I. You, and T. Chung, "Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1077-1088, Mar. 2013.

[17] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF, RFC 3775, Jun. 2004.

[18] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," IETF, RFC 5213, Aug. 2008.

[19] 3GPP TS 29.275, "Proxy Mobile IPv6 (PMIPv6) based Mobilily and Tunneling protocol (Release 11)," stage 3, ver. 10.2.0, Jun. 2011.

[20] T. Trung, Y. Han, H. Choi, and H. Geun, "A Design of Network-based Flow Mobility based on Proy Mobile IPv6," in *Proc. of the 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2011, pp. 373-378.

[21] J. Jang, S. Jeon, Y. Kim, and J. Park, "Resource-Efficient Class-based Flow Mobility Support in PMIPv6 domain," in *Proc. on the 7th International Conference on Networking and Services (ICNS)*, 2011, pp. 166-169.

[22] J. Kim, Y. Morioka, and J. Hagiwara, "An Optimized Seamless IP Flow Mobility Management Architecture for Traffic Offloading," in *Proc. of the 2012 IEEE Network Operations an Management Symposium (NOMS)*, 2012, pp. 229-236.

[23] T. Melia, C. Bernados, A. de la Oliva, F. Guist, and M. Calderon, "IP Flow Mobility in PMIPv6 Based Networks: Solution Design and Experimental Evaluation," *Wireless Personal Communications*, vol. 61, no. 4, pp. 603-627, Dec. 2011.

[24] Fraunhofer FOKUS. (2013, July) Open Evolved Packet Core. [Online]. http://www.openepc.net/index.html

[25] (2013) 3GPP. [Online]. http://www.3gpp.org

[26] 3GPP TR 23.861, "Network based IP flow mobility," ver. 1.7.0, Sep. 2012.

[27] S. Kent and R. Arkinson, "Security Architecture for the Internet," IETF, RFC 2401, Nov. 1998.

[28] 3GPP TS 29.274, "3GPP Evolved Packet System (EPS); Evolved General Packet Radio Service (GPRS) Tunneling Protocol for Control plane (GTPv2-C) (Release 10)," stage 3, ver. 10.6.0, Mar. 2012.

[29] 3GPP TS 24.303, "Mobility management based on Dual-Stack Mobile IPv6 (Release 11)," Stage 3, ver. 11.2.0, Jun. 2012.

[30] 3GPP TR 23.861, "Multi access PDN connectivity and IP flow mobility (Release 9)," ver. 1.3.0, Sep. 2009.

[31] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernstand, and K. Nagami, "Multiple care-of Address Registration," IETF, RFC 5648, Oct. 2009.

[32] G. Tsirtsis, H. Solomon, N. Montavont, G. Giaretta, and K. Kuladinithi, "Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support," IETF, RFC 6089, Jan. 2011.

[33] P. Calhoun, "Diameter Base Protocol," IETF, RFC 3588, Sep. 2003.

[34] C. Kaufman, "Internet Key Exchange (IKEv2)," IETF, RFC 4306, Dec. 2005.

[35] CJ. Bernados, "Proxy Mobile Ipv6 Extensions to Support Flow Mobility," IETF, draft-ietf-netext-pmipv6-flowmob-06, work-in-progress, Feb. 2013.

[36] R. Braden, "Requirements for Internet Hosts -- Communications Layers," IETF, RFC 1122, Oct. 1989.

[37] T. Melia, "Logical Interface Support for multi-mode IP Hosts," IETF, draft-ietf-netext-logical-interface-support-06, work-in-progress, Oct. 2012.

[38] J. Davies. (2007, September) The Cable Guy: Strong and Weak Host Model. [Online]. technet.microsoft.com/en-gb/magazine/2007.09.cableguy.aspx

[39] P. Seite, "Current Practices for Multiple-Interface Hosts," IETF, RFC 6419, Nov. 2011.

[40] Network Simulator 3. [Online]. http://www.nsnam.org/

[41] H. Choi, S. Min, Y. Han, and R. Koodli, "Design and Simulation of a Flow Mobility Scheme Based on Proxy Mobile IPv6," *Journal of Informational Processing Systems*, vol. 8, no. 4, pp. 603-620, 2012.

[42] 3GPP TS 22.278, "Service requirements for the Evolved Packet System (EPS)

(Release 12)," ver. 12.1.0, Sep. 2012.

[43] M. Fiedler, T. Hossfeld, and P. Tran-Gia, "A generic quantitative relationship between quality of experience and quality of service," *IEEE Network*, vol. 24, no. 2, pp. 36-41, Mar. 2010.

[44] A. Oodan, K. Ward, C. Savolaine, M. Daneshmand, and P. Hoath, *Telecommunications Quality of Service Management*, C.J. Hughes, J. O' Reilly, and G. White, Eds. Bodmin, Cornwall, UK: The Institution of Engineering and Technology, 2003, p. 168.

[45] UCT. (2013) University of Cape Town. [Online]. http://www.uct.ac.za/home/

[46] (2013) Fraunhofer FOKUS. [Online]. http://www.fokus.fraunhofer.de/en/fokus/institut/was_ist_fokus/index.html

[47] R. Fielding et al., "Hypertext Transfer Protocol --HTTP/1.1," IETF, RFC 2616, Jun. 1999.

[48] A. Dawson and A. Chadd. (2013, May) Squid: Optimising Web Delivery. [Online]. http://www.squid-cache.org/

[49] (2013, Feb.) The GNU General Public License v3.0 - GNU Project - Free Software Foundation (FSF). [Online]. https://gnu.org/licenses/gpl.html

[50] (2013) myMONSTER. [Online]. http://www.monster-the-client.org/index.html

[51] J. Rosenberg et al., "Session Initiation Protocol (SIP)," IETF, RFC 3261, Jun. 2002.

[52] R. Droms, "Dynamic Host Configuration Protocol," IETF, RFC 2131, Mar. 1997.

[53] J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," IETF, RFC 3315, Jul. 2003.

[54] (2013) netfilter/iptables project homepage - The netfilter.org project. [Online]. http://www.netfilter.org/

[55] Iperf. [Online]. http://iperf.sourceforge.net/

[56] J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach*, 5th ed. USA: Addison-Wesley Publishing Company, 2009.

[57] S. Shakkottai, N. Brownlee, A. Broido, and K. Claffy, "The RTT Distribution of TCP Flows in the Internet and its Impact on TCP based flow control," Cooperative Association for Internet Data Analysis (CAIDA), Tech rep. Mar. 2004.

[58] (2013, July) Wireshark - Go Deep. [Online]. http://www.wireshark.org/

[59] (2013, September) "goodput." (n.d.). [Online]. http://www.yourdictionary.com/goodput

[60] F. Farid, S. Shahrestani, and C. Ruan, "Quality of Service Concerns in Wireless and Cellular Networks," *Communications of the IBIMA*, vol. 2013, p. 15, March 2013.

[61] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Improving the performance of TCP in the Presence of Interacting UDP flows in Ad Hoc Networks," in *Proceesings of NETWORKING*, 2004, pp. 64-75.

[62] L. Balliache. (2012) Practical IP Network QoS. [Online]. www.softwareopal.com/qos/default.php?p=gen102-flows

[63] T. Gopinath, A.S.R. Kumar, and R. Sharma, "Performance Evaluation of TCP and UDP over Wireless Ad-hoc Networks with Varying Traffic Loads," in *2013 Interntional Conference on Communications Systems and Network Technologies (CSNT)* , 2013, pp. 281 - 285.

[64] 3GPP TS 29.281, "General packet Radio System (GPRS) Tunnelling Protocol

User Plane (GTPv1-U)," ver. 11.6.0, Mar. 2013.

[65] stress(1) - Linux man page. [Online]. http://linux.die.net/man/1/stress

[66] The IEEE and The Open Group. (2004) The Open Group Base Specification Issue 6. [Online]. http://pubs.opengroup.org/onlinepubs/009695399/functions/gettimeofday.html

[67] L. Angrisani, G. Ventre, L. Peluso, and A. Tedesco, "Measurements of processing and queuing delays introduced by an open-source router in a single-hop network," *IEEE Transactions on Instrumentation and Measurements*, vol. 55, no. 4, pp. 1065-1076, Aug. 2006.

[68] S. Bradner and J. Mcquaid, "Benchmarking Methodology for Network Interconnect Devices," IETF, RFC 2544, Mar. 1999.

[69] (2012) Stoke Inc. [Online]. www.stoke.com/GetFile.asp?f=f21ae294ea5fcc5b72ee22dc8b31c388

[70] IEEE, "Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater fro 100Mb/s Operation," IEEE, Std 802.3u-1995 (Supplement to ISO/IEC 8802-3:1993; ANSI/IEEE Std 802.3, 1993 Edition), 1995.

[71] Cisco corp. [Online]. www.cisco.com/web/strategy/docs/gov/IPv6perf_wp1f.pdf

[72] H. Zhou, H. Zhang, Y. Qin, H. Wang, and H. Chao, "A Proxy Mobile IPv6 Based Global Mobility Management Architecture and Protocol," *Mobile Networks and Applications*, vol. 15, no. 4, pp. 530-542, Aug. 2010.

[73] H. Hussain, K. Bakar, and S. Sallch, "A Novel Intra-Domain Continues Handover Solution for Inter-Domain Pmipv6 Based Vehicular Network," *International Journal of Advanced Computer Science and Applications*

(IJACSA), vol. 2, no. 12, pp. 12-18, Dec. 2011.

[74] L. Yi, H. Zhou, and H. Zhang, "An Efficient Distributed Mobility Management Scheme Based on PMIPv6," in *Proc. 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2012, pp. 274-279.

[75] A. Chan, H. Yokoto, J. Xie, P. Scite, and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues," *Journal of Communications*, vol. 6, no. 1, pp. 4-15, Feb. 2011.

[76] F. Giust, A. de la Oliva, C. J. Bernados, and R. P. Da Costa, "A network-based localized mobility solution for Distributed Mobility Management," in *14th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2011, pp. 1-5.

[77] M. F. Tsai, N. Chilamkurti, J. H. Park, and C. K. Shieh, "Multi-path transmission control scheme combining bandwidth aggregation and packet scheduling for real-time streaming in multi-path environment," *IET Communications*, vol. 4, no. 8, pp. 937-945, May 2010.

[78] J. C. Fernandez, T. Taleb, M. Guizani, and N. Kato, "Bandwidth Aggregation-Aware Dynamic QoS Negotiation for Real-Time Video Streaming in Next-Generation Wireless Networks," *IEEE Transactions on Multimedia*, vol. 11, no. 6, pp. 1082-1093, Oct. 2009.

[79] S. Kim and S. Lee, "A novel load balancing scheme for PMIPv6-based wireless networks," *International Journal of Electronics and Communication*, vol. 64, no. 6, pp. 579-583, Jun. 2010.

[80] M. Kim and S. Lee, "Load balancing based on layer 3 and IEEE 802.21 frameworks in PMIPv6 networks," in *IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2009, pp. 788-792.

[81] 3GPP TS 24.312, "Access Network Discovery and Selection Function

(ANDSF) Management Object (MO) (Release 12)," ver 12.2.0, Sep. 2013.

[82] 3GPP TS 23.228, "IP Multimedia Subsystem; Stage 2," Stage 2, ver. 12.0.0, Mar. 2013.

[83] S. Deering and R. Hinden, "Internet Protocol Version 6 (IPv6)," IETF, RFC 2460, 1998.

[84] M. Handley, V. Jacobson, and C. Perkins, "SDP: Session Description Protocol," IETF, RFC 4566, 2006.

[85] 3GPP TS 29.214, "Policy and harging Control over Rx reference point (Release 12)," ver. 12.0.0, Jun. 2013.

[86] L. MartinGarcia. (2010) Tcpdump & Libpcap. [Online]. http://www.tcpdump.org/

Appendix A

Background Information and proposed message formats

A.1 Overview of 3GPP's Evolve Packet Core architecture

The EPC was standardised in release 8 of the 3GPP standards and has the following functional entities:

- Packet Data Network Gateway (PDN-GW): Provides access to external Packet Data Networks (PDNs) like the Internet, MNO owned service provisioning platforms (e.g. the 3GPP IP Multimedia Subsystem (IMS) [**82**]) and private corporate IP networks. The PDN-GW provide functionality that includes: IP packet routing and forwarding, UE IP address allocation, uplink and downlink service level charging and is the mobility anchor for inter-system mobility between 3GPP and non-3GPP RANs.
- Serving Gateway (S-GW): Termination point towards E-UTRAN and is the entry point towards the EPC. The S-GW has functionalities that include: IP packet routing and forwarding, packet buffering when the UE is in idle mode, per UE IP-service charging, and is the mobility anchor for intra-3GPP mobility [**2**] i.e. mobility between access networks defined by the 3GPP standardisation body e.g. mobility between UMTS and LTE.
- Mobility Management Entity (MME): The main entity in the EPC for ensuring the reachability of the UE when in idle state (e.g. paging and location management); it is in charge of selecting the gateways (S-GW and PDN-GW) during IP connectivity setup of the UE in a 3GPP access network.
- evolved Packet Data Gateway (ePDG) [**4**]: The gateway providing access to the EPC from non-3GPP RANs (e.g. WLAN); it is in charge of performing packet encapsulation/de-capsulation of packets for IPSec [**27**] (security association between the UE and the ePDG), enforcing QoS policies and charging, and IP packet routing and forwarding between the PDN-GW and the UE [**4**].

- Home Subscriber Server (HSS) and Access Authentication Authorization (AAA) server: The HSS and AAA are responsible for storing user subscription information and for providing security measures to ensure that the UE is authorised to access the EPC network.
- Policy and Charging Control (PCC) architecture [**11**]: The PCC establishes the QoS rules and is the MNO policy provisioning architecture that is in charge of ensuring that the UE service sessions are provided with the appropriate transport (in terms of bandwidth and Quality of Service (QoS) treatment [**11**]) and charging and billing. The PCC has a Policy and Charging Rules Function (PCRF), Policy and Charging Enforcement Function (PCEF) and the Bearer Binding and Event Reporting Function (BBERF) as functional entities. The PCRF is the policy control entity of the PCC. The PCEF and BBERF enforce the policies set forth by the PCRF for downlink and uplink traffic of the end-users. The PCEF resides in the PDN-GW and the BBERF resides in the access gateways (S-GW, ePDG, etc).
- Access Network Discovery and Selection Function (ANDSF): A server residing in the EPC for providing inter-system mobility policies to the UE and informing the UE of the available RANs in the vicinity of the UE. The UE uses these policies and information for network selection or mobility.

Figure A.1 illustrates the non-roaming architecture of the EPC.

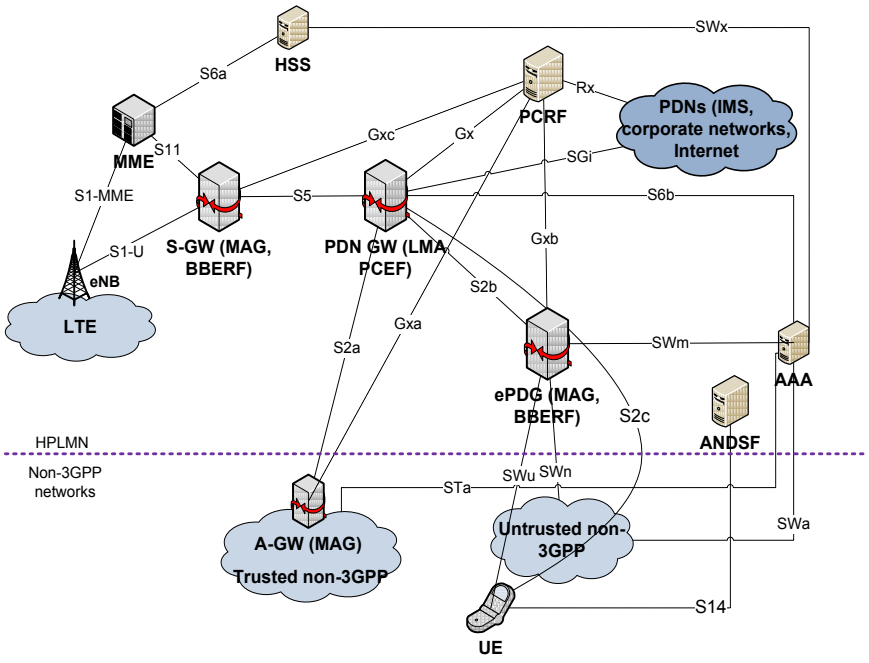

Figure A.1: 3GPPs Evolved Packet Core network [4]

A.2 Overview of the PBU mobility message format

In order to carry the Mobile Internet Protocol version 6 (MIPv6) messages IETF defined a new IPv6 extension header, called Mobility Header (MH) [**17**]. In IPv6 networking, the IPv6 packets consist of an IPv6 header and a payload. The IPv6 header has parameters such as source IP address, destination IP address, traffic class, payload length, and next header field, and is used by IPv6 network nodes to process the packets for routing purposes. In IPv6, additional information can be encoded in what is called extension headers [**83**]. An extension header is an additional header that is placed between the IPv6 header and the upper-layer header in an IPv6 packet, and is identified by a distinct next header value [**83**]. Unlike IPv6 headers, that are examined and processed by each IPv6 node along the delivery path, extension headers are only examined or processed by the node identified by the destination IP address in the IPv6 header. The MH is identified by a next header field of 135, and has the following header fields: MH type, Reserved field, Checksum and a Message data field [**17**].

The MH type field identifies the particular MIPv6 message e.g. a BU or BA message [**10**]. The Checksum field contains a checksum of the MH, and the Message data field, contains the information specific to the MH type e.g. HoA and CoA. The MIPv6 protocol also defines mobility options within the messages, but can only be added after the fixed portion of the Message data. An example of a mobility option is the Home Network Prefix [**18**] option. This option is used to indicate the HNP of the UE. Figures A.2 and A.3 illustrate the MH and the BU message format.

The various flags (A, H, L, K, etc.) in figure A.4 are used for different purposes. The P flag is used by the PMIPv6 mobility protocol to indicate that the message is for a PBU message

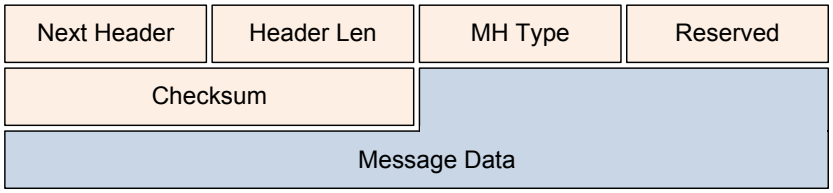

Figure A.2: MIPv6 Mobility Header

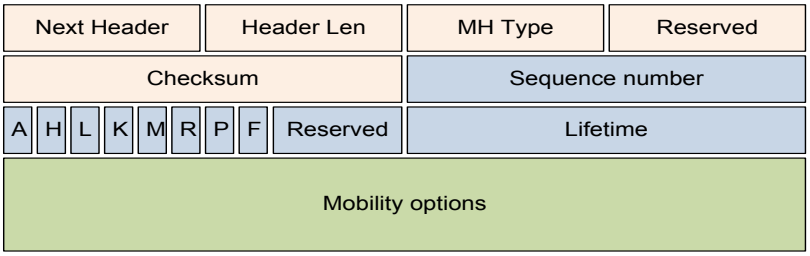

Figure A.3: MIPv6 Binding Update message

A.3 Format of the proposed Additional Route mobility option

An additional mobility option, called Additional Route, is defined for the PBA message. This mobility option is used for sending the HNPs of the UE"s additional connections to the access gateways (S-GW, ePDG). The mobility option has a similar format to the standard HNP mobility option [**18**] of the PBU/PBA messages. The HNP contained in this mobility option should not be sent to the UE and are exclusively for the access gateways only. The mobility option has the format as shown in figure A.4, and the fields are defined as follows:

- Type: An 8-bit field indicating to the receiving entity (the MAG in the access gateways) that it is an Additional Route mobility option.
- Length: An 8-bit integer indicating the length of the mobility option in octets (this value is excluding the type and length fields). This value should be set to 18.
- Reserved: An unused 8-bit field that must be initialised to zero by the LMA and be ignored by the MAG.
- Prefix length: An 8-bit integer indicating the HNP length contained in the option.
- Home Network Prefix: A 16-byte field containing an additional HNP belonging to the UE.

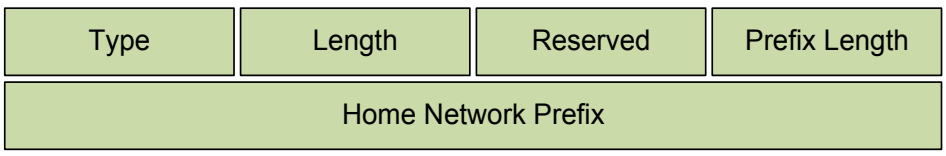

Figure A.4: Format of the Additional Route mobility option

A.4 Format of the proposed Routing Rule mobility option

In order to send the routing filters to the LMA a new mobility option, called Routing Rule mobility option is defined for the PBU and PBA messages. The MAG appends and sends the in a PBU message in order to request for the creation, modification, or removal a flow binding. The LMA also appends the option to the PBA message for informing the MAG on the outcome of the request. The format of the Routing Rule mobility option is shown in figure A.5; each field is defined as follows:

- Type: An 8-bit integer value indicating that the mobility option is a Routing Rule mobility option.
- Length: length of the mobility option in octets.
- Flags (A-C): The A-flag is set to 1 in order to indicate that the request is for creating a new flow binding, and set to 0 otherwise. The B-flag is set 1 when requesting to delete the flow binding matching the parameters in the mobility option, and is set to 0 otherwise. The C-flag is set to 1 when requesting to update a flow binding and set to 0 otherwise. The update only allows changing the HNP belonging to a routing filter.
- Home Network Prefix: The HNP to which the routing filter should be bound. The MAG is not necessary aware of this HNP.
- Source and destination IP address: 128 bit field containing the source and destination IPv6 IP addresses to be matched to data packets. The source IP address is the IP address of the sender and the destination IP address is the HoA configured from the HNP on the interface of the UE.
- Source and destination port: 16-bit source and destination port numbers to be matched for the data packets sent to the UE from a sender node, where the source port is the port of the sender node and the destination port is the port used by the application on the UE.
- D-flag: This flag indicates the type of transport protocol used by the application. Only TCP or UDP is supported, since it is the most common transport protocol used in the Internet and applications. When the D-flag is set to 1, the transport protocol used is TCP. UDP is used when the flag is not set to 1.
- Status: An 8-bit integer indicating the success or failure of the flow binding operation. The status value is only set by the LMA in the PBA message. A status value set to 0 means that the flow operation was carried out successfully by the LMA, and if set to a value other than 0 implies that the operation was unsuccessful.

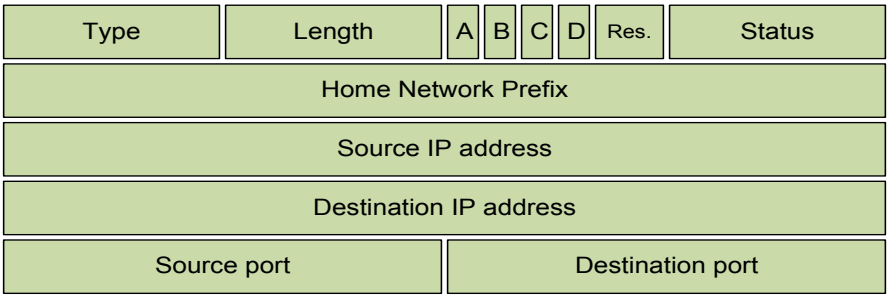

Figure A.5: Format of the proposed Routing Rule mobility option

Appendix B

Hardware Specifications of the Evaluation Framework

The evaluation framework described in chapter 4 comprises entirely of commercially available equipment. Each of the EPC nodes is implemented on a desktop computer. The hardware specifications of the desktop computers are listed in table B.1. Table B.2 summarises the complete list of hardware used in the evaluation framework.

Table B.1: Hardware specifications for the EPC node desktop computers

	PDN-GW, S-GW, ePDG, eNodeB, UE, MME, Enablers
Processor	4x Intel (R) Core (TM) i3-2100
CPU	3100.00 MHz
Cache size	3072 kb
RAM	2028344kB – 2028352 kB
Operatng System (OS)	Ubuntu distribution 11.04 LTS
OS kernel	Linux 2.6.38-13-generic (i686)

Table B.2: Summarised list of hardware used in the evaluation framework

Hardware	Model	Quantity
PDN-GW, S-GW, ePDG, eNodeB, UE, MME, Enablers	Desktop Computer	7
8-port Ethernet switch	Trendnet 10/100 Mbps	5
802.11 WiFi Access Point	D-Link DAP-1155 Wireless N150	1
Ethernet network adapters	D-Link DGE-528T Gigabit Ethernet Adapter	7

	Realtek RTL8111/8168B PCIExpress Gigabit Ethernet Adapter	7
	VIA Technologies VT6105/VT6106S [Rhine-III] onboard Ethernet Adapter	7

Appendix C

The OpenEPC adaptive video streaming function and UE tools

The OpenEPC Toolkit offers a series of application functions for showcasing the capabilities of the OpenEPC. These application functions are all pre-configured to work straight out of the box. One in particular application function of interest is the Adaptive Video Streaming application function.

C.1 Adaptive Video Streaming

The OpenEPC deploys a Media Delivery Function (MDF) for demonstrating an adaptive video streaming scenario in the OpenEPC. The MDF is housed in the OpenEPC enablers and has a network interfaces to the internal network (net_a) with IP address fc00:1234:1::41.

The MDF is controlled with a Session Initiation Protocol (SIP) interface; a SIP call is placed to the MDF in order to request content. The initial call‟s INVITE [**51**] message contains the content Identity (ID) set in the Session Description Protocol (SDP) [**84**] payload. An INVITE message is a SIP method used for specifying the action the sender (the end-user) wants the receiver (the MDF) to perform; In this case, the end-user wants the MDF to start a video stream. The INVITE request contains information like the IP address of the MDF, the UE‟s IP address and the type of session the user wishes to establish. SDP is a format describing the streaming media initialisation parameters and is used between communication peers for negotiating the session parameters; refer to [**84**] for description of SDP. The default bandwidth in the SDP payload is set to 300 kbps. The MDF will check whether a content session is available for the content ID received. If the content session is available, the MDF sends an AA-Request (AAR) [**85**] Diameter message over the Rx interface towards the PCRF to request for resource allocation. The AAR Diameter message is also used to provide the PCRF with the session information e.g. the end-users‟ SIP Uniform Resource Identifier (URI), bandwidth, content ID etc. A full list of information is specified in the 3GPP specification [**85**]. The SIP URI is the SIP identity of the end-user and has a similar format to

an email address e.g. sip:alice@openepc.test, where alice is the host name and openepc.test is the domain of the SIP service provider (the OpenEPC domain name).The PCRF verifies whether the end-user with the SIP URI is allowed in the network. If allowed, the PCRF will generate PCC rules based on the end-user profile and push the rules to the PCEF in the PDN-GW and the BBERF in the access gateways (S-GW and ePDG). If the bandwidth allocation for the end-user was successful, the PCRF sends the MDF an AA-Answer (AAA) [**85**] Diameter message with a status set to successful. The MDF then replies with a SIP message to the UE with 200 OK [**51**] status and the SDP payload specifies the necessary data for retrieving the video stream. Figure C.1 illustrates the procedure described above between the MDF and interaction with the PCRF.

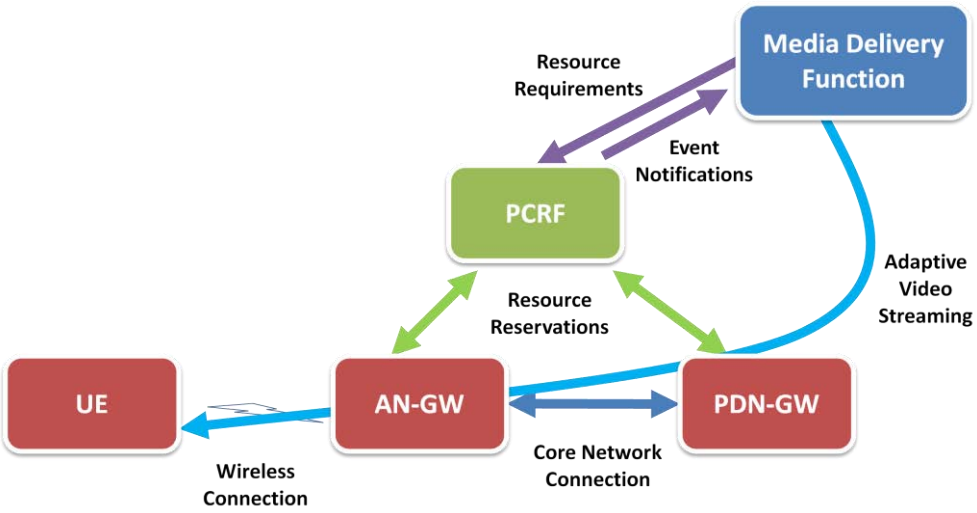

Figure C.1: Adaptive video streaming: Interaction between the MDF and PCRF [24]

To stop the video stream, a BYE [**51**] message is sent to the MDF. The MDF then sends a Session Termination Request (STR) [**85**] Diameter message to the PCRF to terminate the established video streaming session. This results in the PCRF removing the PCC rules of the session and notifying the PCEF and BBERF. The PCRF replies to the MDF with a Session Termination Answer (STA) [**85**] Diameter message of the successful removal of the resources and the MDF stops the video stream.

C.2 The UE myMONSTER tool

The myMONSTER tool is developed by Fraunhofer FOKUS and is a SIP client on the UE machine. The tool is written in Java programming language and can be installed on the Linux OS. The tool can be used for making IMS calls and allows the end-user to request the MDF

for video streams.

To use the myMONSTER tool the end-user has to create a profile. The client machines are pre-provisioned with two end-user credentials (Alice and Bob) with each having three profiles: IMS with PCC, IMS without PCC and Videodemo profile. Only the latter profile is considered in this research. Figure C.2 shows the myMONSTER GUI and the profiles defined for Alice.

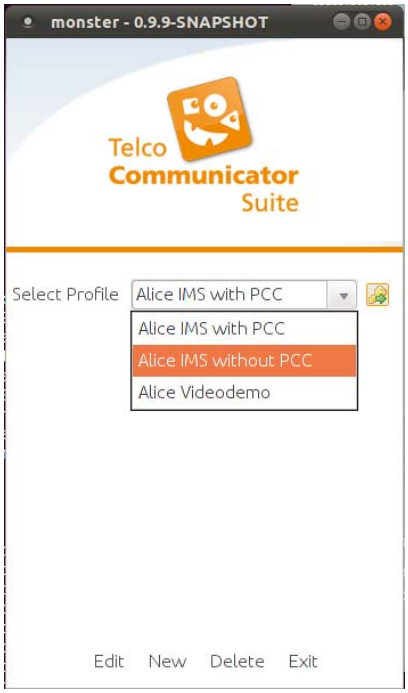

Figure C.2: The myMONSTER graphical user interface in the UE

Clicking the connect button in the myMONSTER tool with the Videodemo profile set (refer to figure C.3) will generate a SIP call to the MDF for a video stream to start. The myMONSTER tool is directly connected to the MDF after the SIP call is a success.

Figure C.3: Alice registering with the videodemo profile to the MDF

The end-user can now start video stream by clicking the videodemo button as shown in the figure C.4a. Clicking the videodemo button will open another window (figure C.4b) that enables the video stream to be played or stopped. The SIP URI is used as remote URI in the call to the MDF.

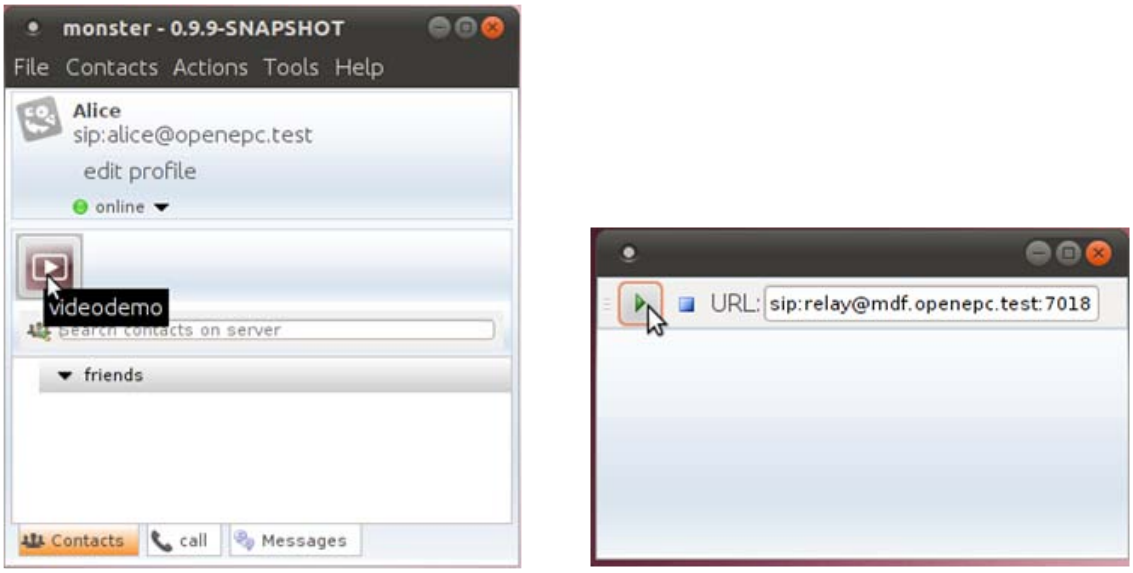

Figure C.4: (a) Alice clicking on the videodemo button to start the video stream from the MDF and (b) Stopping and starting the video stream

C.3 The UE Mobility Manager Graphical User Interface tool

The MM GUI (as shown in figure C.5) is written in Java programming language and is used to interact with the MM on the UE. The MM GUI, when started on the UE, will show a list of all the available access networks that the UE can attach to. The MM GUI contains various buttons that can be toggled for various purposes. For example, the management (Mgmt) toggle button will manual only handover or automatic handovers through the use of inter-system mobility policies from the network. The IPv4 and IPv6 toggle buttons is used to choose the preferred IP version used for the IP address requests. The default operation assumes IPv4.

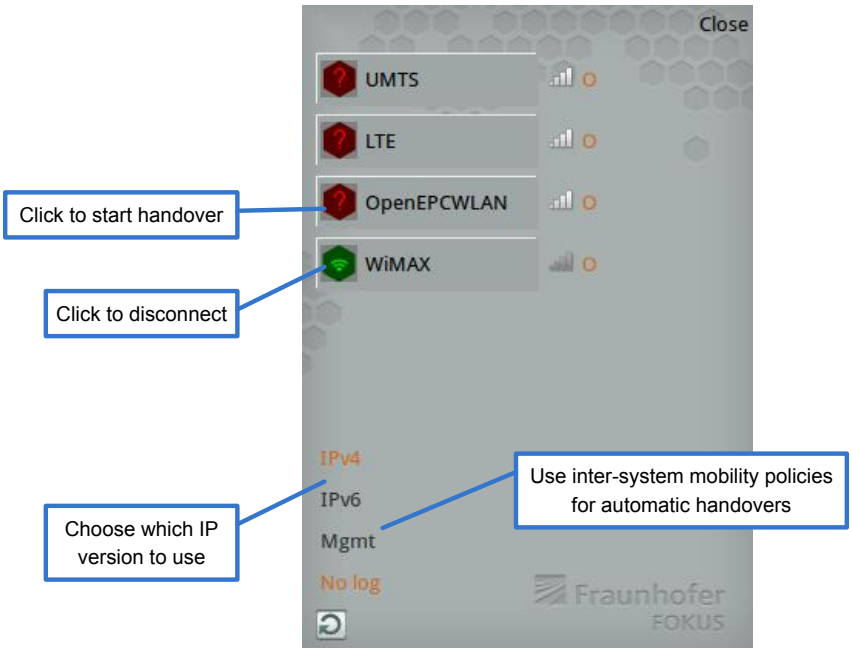

Figure C.5: The MM graphical user interface in the UE

Appendix D

Enhancements to PMIPv6 for IP flow mobility

D.1 LMA PBA creation procedure enhancement

The functionality of the LMA is achieved through various procedures [**19**] [**18**] e.g. there are procedures for processing the PBU/PBA mobility messages, carry out the UE initial attach requests, carry out handover events, and a procedure to create and send the PBA messages, etc. From these procedures, the PBA creation procedure is enhanced to enable the LMA to search for and send any additional HNPs belonging to a particular UE in a PBA message. Enhancing the PBA creation procedure does not affect any other LMA procedure since it is the last procedure performed after the other procedures. The proposed enhancements are discussed below and a summary given in a flow chart of figure D.1:

- The LMA has to search for any additional Binding Cache Entries (binding cache entries) of the UE, using as the binding cache entry lookup key: the UE‟s International Mobile Subscriber Identity (IMSI), Access Point Name (APN) and searching for entries where the HNP is not the same as the HNP of the PBA. This will ensure that the UE‟s binding cache entries for the other access networks are selected and not the one where the PBA is being sent to since the target access gateway (with the MAG functionality) will already receive the new HNP in the PBA.
- To ensure that the HNPs are all unique, if the LMA finds additional binding cache entries for the UE, it should extract and compare the HNPs against the new allocated HNP. This will ensure that LMA send only unique HNPs to the access gateways and thus avoiding them creating multiple routes of the same HNP.
- If any of the extracted HNPs are the same as the new HNP, the LMA should not send them in the PBA message, but should add the remaining HNPs to the PBA message in the Additional Route mobility option. The LMA appends the Additional Route mobility option to PBA message for sending any of the HNPs of the UE‟s additional connections to the access gateways (S-GW, ePDG). The HNP contained in this mobility option should not be sent to the UE and are exclusively for the access

gateways only. The format of the Additional Route mobility option is detailed in Appendix A.3.

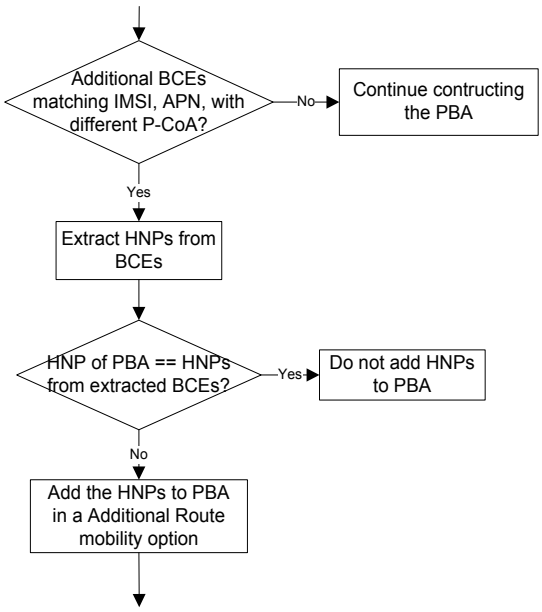

Figure D.1: Enhancement to the PBA creation procedure of the LMA functionality

The pseudo code for the implementation of the above enhancements is:

```
1   mip_opt_ipv4_home_address second_route;

2   int count = 0;
3   binding_entry_t *binding2=0;
4   int ATT = 0;            //added this to store the int value of ATT

5   att.att=bce->att;
6   ATT = (int)(att.att);

7   count = count_bindings(bce->id);            //Added by charna

8   switch(count)           //Switch added by charna
9   {
10              case 0:
11                      LOG(L_DBG,"No additional route found for client, first attach\n");
12                      break;
13              case 1:
14                      binding2 = lma_get_binding_not_att(bce->id,bce->apn, bce->ai_family, ATT);
15                      if (binding2){          //binding is not the one provided to this function
16                              if(!ip_address_cmp(bce->ha, binding2->ha)){          //compare the addresses again to make sure
                                                                                    //IP addresses the same, so dont send to MAG
17                                      LOG(L_DBG, "Not appending HNP/HoA to PBA for the MAG\n");
18                              } else {    //The HNP/HA was different do adding it to the PBA
19                                      memcpy(&second_route.hA, &(binding2->ha.ip.v4.s_addr), 4);
```

```
20                                          mo=mip_bind->mip_new_opt_typed
(MIP_Opt_Type_IPv4_Home_Address,&second_route);
21                                          mip_bind->mip_add_opt_to_list(&pba->opt,mo);
22                                  }
23                          } else { //The same binding parsed to this function
24                                  LOG(L_DBG,"No additionl route found for client\n");
25                          }
26                          break;
27                  case 2:
28                          binding2 = lma_get_binding_not_att(bce->id,bce->apn, bce->ai_family, ATT);
29                          if(binding2){//failsafe, already know there is a binding for the client
30                                  memcpy(&second_route.hA, &(binding2->ha.ip.v4.s_addr), 4);
31                                  mo=mip_bind->mip_new_opt_typed(MIP_Opt_Type_IPv4_Home_Address,&second_route);
32                                  mip_bind->mip_add_opt_to_list(&pba->opt,mo);
33                                  LOG(L_DBG, "Appending other HNP/HoA of client to PBA for the MAG\n");
34                          } else {
35                                  LOG(L_DBG,"False positive\n");
36                          }
37                          break;
38                  default:
39                          LOG(L_ERR, "Wrong AI family for the BCE when trying to send the PBA: [%d]\n", bce->ai_family);
40                          break;
41  }
```

The enhancements are made the *create_and_send_PBA(uint8_t status,unsigned int handoff_indication, binding_entry_t *bce,ip_address ip_dst,ip_address ip_src,uint32_t ul_gre_key)* function of lma.c

D.2 LMA PBU message processing procedure enhancement

For the LMA to create, modify or delete entries in the flow binding list or process the Routing Rule mobility options, requires enhancements to the default PBU message processing procedure. The procedure is enhanced with the following additional steps (refer to figure D.2 for a flow diagram illustrating the enhancements discussed below):

- The LMA has to check whether a Routing Rule mobility option exist in the PBU message by checking the Type field in the mobility option. If the option exists the LMA should check the flags in the mobility option header to determine whether the mobility option is a request for creating, deleting or updating a flow binding.
- If the request is for creating a new flow binding, the LMA has to check whether the binding cache entry has a flow binding list. If no flow binding list exist, A flow binding list with the requested flow binding should be created. However, if a flow

binding list is present, the LMA should compare the routing filter of the mobility option to the routing filters of the flow binding entry in order to determine whether the flow binding has been created previously for the HNP received in the mobility option. This check is performed to prevent the creation of duplicate flow binding entries. If the routing filters differ for any of the parameters, the LMA should create the flow binding, otherwise request should be ignored, since the flow binding already exists.

- If the request is for the removal of a flow binding, the LMA has to check whether the binding cache entry has a flow binding list. If there is no flow binding list, the request should be ignore since there is nothing to delete, otherwise the LMA should extract the flow binding list and check whether a flow binding entry exists for the HNP received in the mobility option. If no entry is found the request should be ignored otherwise the routing filter of the mobility option should be matched against the routing filters of the flow binding entry in order to find the correct routing filter to delete. If no match is found between the routing filters, the request should be ignored since the flow binding does not exist, otherwise the LMA should delete the flow binding.
- If the request is for updating a flow binding, the LMA should check whether a flow binding list exist for the UE, and if no list exist, the request should be ignore since there is nothing to update. If on the other hand a flow binding list do exist, the LMA should match the routing filter of the of mobility option to all the routing filters in the flow binding list in order to find the flow binding entry to update. If none of the routing filters match, the LMA should ignore the request since there is no existing entry to update, otherwise the LMA should compared the HNP corresponding to that matched routing filter to the HNP of the mobility option in order to determine whether the flow binding has been updated. If the HNPs are the same, the LMA should ignore the request since the entry is already updated, otherwise the LMA should update the flow binding entry by replacing the HNP associated to the routing filter with the HNP received in the mobility option.

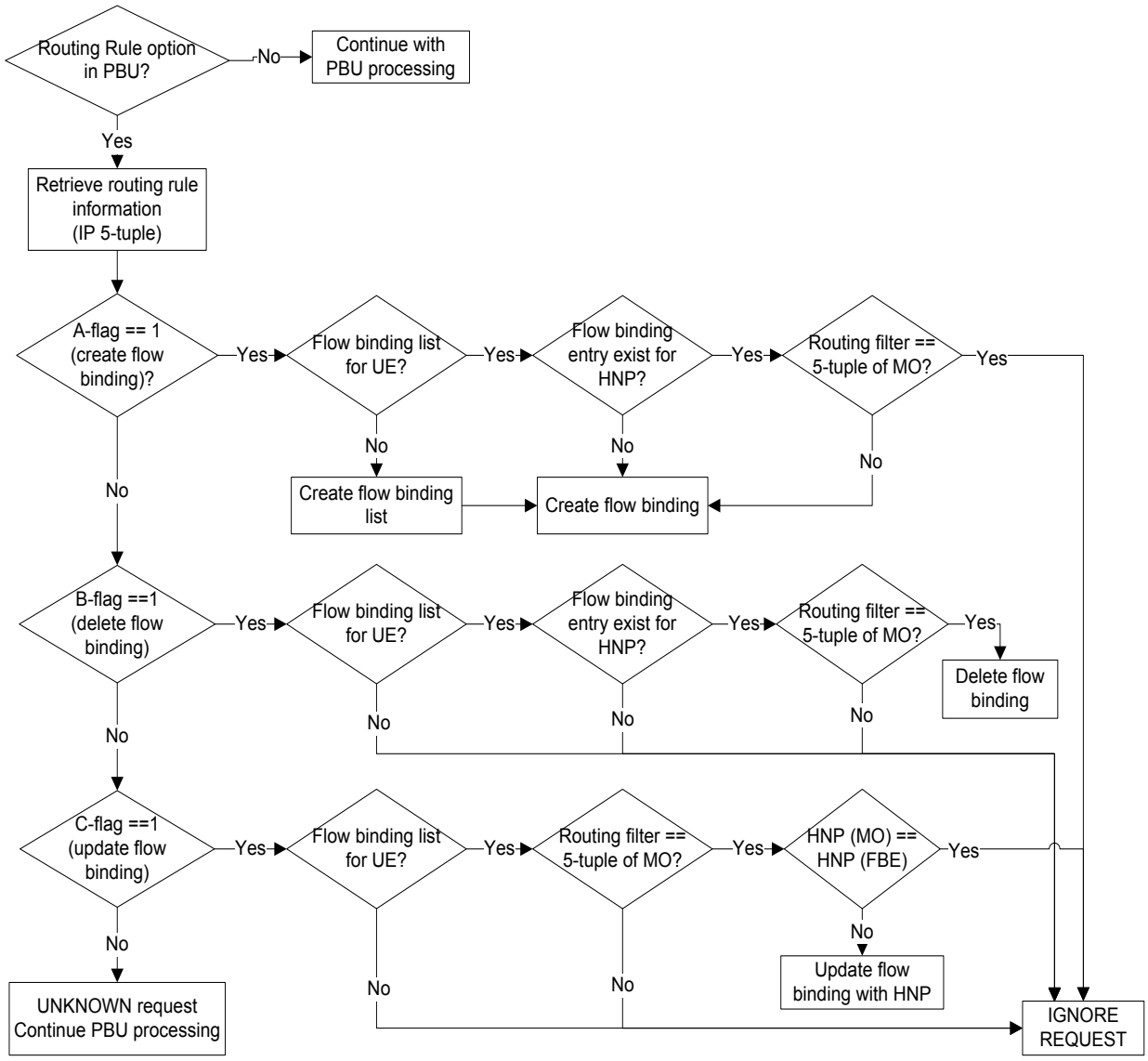

Figure D.2: Enhancement to the PBU message processing procedure of the LMA

The pseudo code of the implementation in the OpenEPC code is:

```
1   temp = mip_bind->mip_get_opt_from_list(&options, MIP_Opt_Type_Routing_Rule, NULL);  //Retrieve routing rule from the PBU
2   if (temp) {
3               LOG(L_DBG, "Routing Rule option found\n");
4               routing_rule = &temp->opt.routing_rule;
                //Copy the received IPs to the IP holders declared
5               memcpy(&src_ip.s_addr,routing_rule->src_addr,4*sizeof(uint8_t));
6               memcpy(&dst_ip.s_addr,routing_rule->dst_addr,4*sizeof(uint8_t));
7               memcpy(&gw_ip.s6_addr,routing_rule->routable_addr,16*sizeof(uint8_t));
8               switch (routing_rule->intension)
9               {
10                      case 0:     //add routing rule
11                                  routing = lma_get_routing_rule(routing_rule->protocol, src_ip, dst_ip, routing_rule->src_port,
    routing_rule->dst_port);        //First check if this routing rule already exists
12                                  if ( no routing rule){   //No routing rule found, create and add the routing rule
```

```
13                                      routing = lma_new_routing(&(routing_rule->protocol),&src_ip, &dst_ip, routing_rule->src_port, routing_rule->dst_port, &gw_ip);          //Formulate the routing rule entry
14                                      added_rule = lma_add_routing_rule(routing);          //Add the routing rule
15                                      if (added_rule) {       //Routing rule was successfully added to the routing rules list
16                                              ip_address_print_comment(L_DBG,"Source IP", src_ip);
17                                              LOG(L_DBG,"Source port %d\n", routing_rule->src_port);
18                                              LOG(L_DBG,"Destination port %d\n", routing_rule->dst_port);
19                                      } else {
20                                              LOG (L_DBG, "Routing not added to routing rules list\n");
21                                      }
22                              } else { //Routing rule exists in the routing rule list
23                                      LOG (L_DBG, "Routing rule already exist, ignoring request to add routing rule\n");
24                              }
25                              break;
26                      case 1:     //Update a routing rule
27                              routing = lma_get_routing_rule(routing_rule->protocol, src_ip, dst_ip, routing_rule->src_port, routing_rule->dst_port); //Get the routing rule to update
28                              if (!routing){          //Routing rule does not exist
29                                      LOG (L_DBG, "Routing rule does not exist, ignoring request to update\n");
30                              } else {
31                                      updated_rule = lma_update_routing_rule (routing, &gw_ip);       //Update the routing rule
32                                      if(updated_rule){       //Update was a success
33                                              LOG (L_DBG, "Routing rule succesfully updated\n");
34                                      } else {
35                                              LOG (L_DBG, "Routing rule was not updated\n");
36                                      }
37                              }
38                              break;
39                      case 2: //del a routing rule
40                              routing = lma_get_routing_rule(routing_rule->protocol, src_ip, dst_ip, routing_rule->src_port, routing_rule->dst_port); //Get the routing rule to delete
41                              if (!routing){          //Routing rule does not exist
42                                      LOG (L_DBG, "Routing rule does not exist, ignoring request to delete\n");
43                              } else {
44                                      updated_rule = lma_del_routing_rule (routing);          //Update the routing rule
45                                      if(updated_rule){       //Delete was a success
46                                              LOG (L_DBG, "Routing rule succesfully deleted\n");
47                                      } else {
48                                              LOG (L_DBG, "Routing rule was not deleted\n");
49                                      }
50                              }
51                              break;
52                      default:
53                              LOG(L_ERR, "ERROR");
54                              break;
55              }
56      } else {
57              LOG(L_DBG, "No routing rule option found\n");
58      }
```

D.3 LMA packet processing procedure enhancement

Normally when downlink packets arrive at the PDN-GW/LMA and addressed to the HoA of the UE, the LMA would extract the packet header and search for a binding cache entry matching the HNP of the destination IP address of the packet. If the LMA finds a binding cache entry it forwards the packet to the P-CoA of the binding cache entry or drop the packet if no forwarding route can be determined. In the proposed solution, the LMA has to consider the routing filters in the flow binding list in order to forward the packets to a specific P-CoA. The following enhancements are proposed to the basic packet processing procedure to achieve flow-based routing:

- After a binding cache entry has been located for the downlink packet, the LMA has to check if a flow binding list is associated to the binding cache entry. If no flow binding list exists, the LMA should just forward the packet to the P-CoA of the binding cache entry otherwise the LMA should search the flow binding list for a flow binding entry by matching the IP 5-tuple of the packet header to the routing filters in the flow binding list.
- If a flow binding entry exists, the LMA should compare the HNP of the entry to the HNP of the extracted binding cache entry, and if the same, forward the packet to the P-CoA of that binding cache entry, otherwise, search for additional binding cache entries of the UE and using the IMSI as the binding cache lookup key. The IMSI is used as look-up key since it is the only parameter that all the binding cache entries of a specific UE have in common, and would thus yield all the binding cache entries belonging to the UE.
- If the UE has additional binding cache entries, the LMA should compare the HNP of the flow binding entry to the HNPs of the binding cache entries and forward the packet to the P-CoA of the binding cache entry that yields a match. However, if the HNP matches none of the HNPs in the additional binding cache entries or if the UE has no additional binding cache entries, the LMA should forward the packet to the P-CoA of the original binding cache entry (i.e. the binding cache entry extracted using the HNP of the destination IP address of the packet). This means that there was no flow binding created for the HNP.

Figure D.3 illustrates a flow diagram of the standardised packet processing procedure and the

proposed enhancements (highlighted in blue) as outlined in the previous discussion.

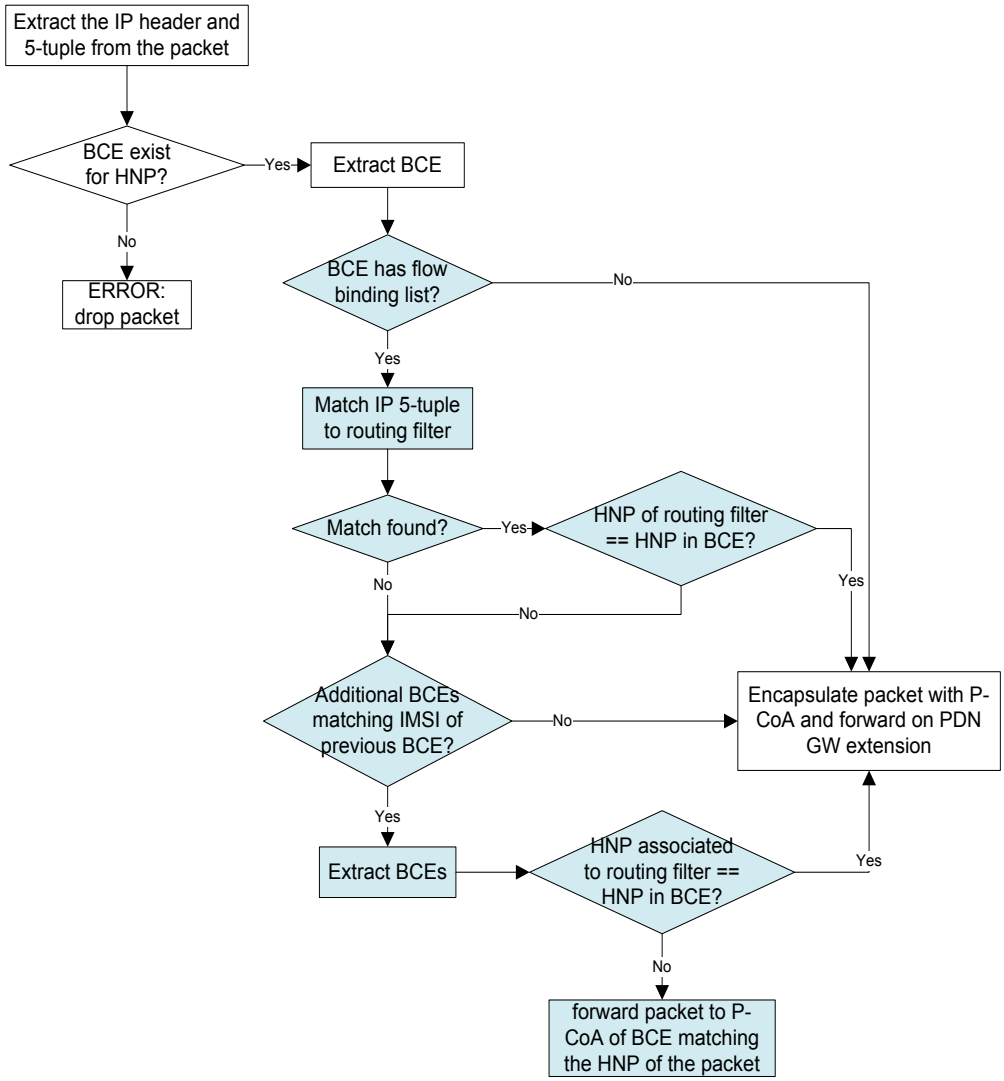

Figure D.3: Packet processing enhancements for flow based routing

The pseudo code of the algorithm implemented in the OpenEPC packet_handler function is:

```
1   packet_handler (uint8_t *packet, int len, uint32_t teid, uint8_t extension)
2   {
3           struct ip* hdr; src_route_t *source_route = 0; dst_route_t *destination_route = 0; host_route_t *host_route = 0;
4           extension_pipe_msg_t *message = 0; routing_entry_t *rule=0;

6           str *s_protocol= 0; uint16_t src_port=0, dst_port=0; struct tcphdr* tcp_header = 0; struct udphdr* udp_header = 0;

7           packet header = (struct ip*) packet;
8           ip_address source, destination;
9           set source.ip = packet_header->ip_src;
10          set destination.ip= packet_header->ip_dst;

11          if (binding){
```

```
12                      if (packet header == IPPROTO_UDP) {
13                              transport_protocol = “udp”;
14                              udp_header = (struct udphdr*)(packet+sizeof(struct iphdr));
15                              source_port = udp_header->source;
16                              destination_port = udp_header->destination;

17                      } else if (packet header == IPPROTO_TCP) {
18                              transport protocol = “tcp”;
19                              tcp_header = (struct tcphdr*)(packet+sizeof(struct iphdr));
20                              src_port = tcp_header->source;
21                              dst_port = tcp_header->dest;
22                      }
23                              source_route = match_src_route(PDNGW.extension[extension] ->source route_table, source);
24                              if (no source_route) goto error;
25                              print_source_route(L_DBG, source_route, extension);

26                              if (source route->flags & ROUTING_USE_HOST_SOURCE_ROUTING) {
27                                      LOG_ROUTE(L_DBG, "Using host routing table for source\n");
28                                      host route = match_host_route(source);
29                                      if (no host_route) {
30                                              goto error;
31                                      }
32                                      print_host_route(L_DBG, host_route);
33                              } else {
34                                      destination_route = match_dst_route(PDNGW.extensions[source_route->ext]->
    destination_route_table, destination);
35                                      if (no destination_route) {
36                                              goto error;
37                                      }
38                                      print_dest_route(L_DBG, destination_route, source_route->ext);
39                                      if (destination_route->flags & ROUTING_USE_HOST_DEST_ROUTING) {
40                                              LOG_ROUTE(L_DBG, "Using host routing table for destination\n");
41                                              host_route = match_host_route(destination);
42                                              if (no host_route) {
43                                                      LOG_ROUTE(L_DBG, "Using default destination route\n");
44                                                      if (PDNGW.extensions [source_route->ext]-
    >destination_route_table->def) {
45                                                              destination_route = PDNGW.extensions [source_route-
    >ext]->destination_route_table->default;
46                                                              print_dest_route(L_DBG, destination route, source
    route->ext);
47                                                      }
48                                                      else goto error;
49                                              }
50                                              print_host_route(L_DBG, host_route);
51                                      }
52                              }
53                              message = shm_malloc(sizeof(extension_pipe_msg_t));
54                              if (!message) {
55                                      LOG(L_ERR, "Could not allocate memory for pipe message\n");
```

```
56                                      goto error;
57                              }
58                              bzero(msg, sizeof(extension_pipe_msg_t));
59                              msg->packet = shm_malloc(sizeof(uint8_t)*len);
60                              if (!(msg->packet)) {
61                                      LOG(L_ERR, "Could not allocate memory for pipe message payload\n");
62                                      goto error;
63                              }
64                              memcpy(message->packet, packet, len);
65                              msg->ai_family = AF_INET;
66                              if (hr) {
67                                      LOG(L_DBG, "Searching for routing rule\n");
68                                      binding->routing_rule_match(*s_protocol,src,dst,src_port,dst_port,&rule);
69                                      if (rule){
70                                              LOG(L_DBG, "Rule found, now implementing routing rule\n");
71                                              message->dst = rule->gateway_ip;
72                                              message->teid = hr->teid;
73                                      } else {
74                                      message->dst = host_route->gateway;
75                                      message->teid = host_route->teid;
76                                      }
77                              } else {
78                                      message->destination = destination_route->gateway;
79                                      message->teid = destination_route->teid;
80                              }

81                              message->len = len;

82                              if (hr) {
83                                      LOG_ROUTE(L_DBG, "Sending packet using host route\n");
84                                      PDNGW.extensions[host_route->ext]->bind->send(PDNGW.extensions[host_route-
    >ext]->send_pipe, message);
85                              } else {
86                                      LOG_ROUTE(L_DBG, "Sending packet using destination route\n");
87                                      PDNGW.extensions[source_route->ext]->bind-
    >send(PDNGW.extensions[source_route->ext]->send_pipe, message);
88                              }

89                              return 1;
90              }
91      error:
92              if (message) {
93                      if (message->packet) shm_free(msg->packet);
94                      shm_free(message);
95              }
96              return 0;
97      }
```

D.4 MAG PBA message processing procedure enhancement

Similar to the LMA functionality, the MAG functionality also has various procedures. In this research, the PBA message processing procedure of the MAG is enhanced in order to process the proposed Additional Route mobility option and create the routes corresponding to the received HNPs. The proposed enhancements are:

- The MAG has to check for an Additional Route mobility option in the PBA message, and if the option is present, extract the option and check whether a HNP is present. If no HNP is present, the MAG should skip processing this option and continue processing the rest of the PBA message.
- If a HNP is present, the MAG should extract and create an entry in its binding update list [**18**] for the additional HNP, and populate the entry with the information (IMSI, APN, etc) in the PBA message. This step assumes that the HNP received in the option is different to the HNP received in the standard HNP mobility option of the PBA message. No entry should exist in the binding having the same HNP, since routing is performed by matching the HNP of received packets to entries in the binding update list. If multiple entries exist having the same HNP, the MAG would not be able to choose the entry to find the forward path for packets addressed to the UE.

The pseudo code for the implementation of the above enhancement is:

```
1   mip_opt_ipv4_home_address *other_address=0;
2   bzero(&other_ip_route, sizeof(ip_address));
3   temp = mip_bind->mip_get_opt_from_list(&options, MIP_Opt_Type_IPv4_Home_Address, NULL);
4   if (temp) {
5           other_address = &temp->opt.ip4_home_addr;

6           if (other_address){
7                   LOG(L_DBG,"Received an aditional route for MNI [%.*s], adding to the routing table\n",
    mobile_node_identifier->identifier.len,mobile_node_identifier->identifier.s);
8                   memcpy(&other_ip_route.ip.v4.s_addr,other_address->hA,4*sizeof(uint8_t));
9                   other_ip_route.ai_family=AF_INET;
10                  mag_add_other_routes(&other_ip_route, &(binding->current_lma));
11          } else {
12                  LOG(L_DBG, "Received an additional routing option in the PBA, but the routing address is not set");
13          }
14  }
```

The enhancements are made in the *process_proxy_binding_acknowledgment (mip_binding_ack *m,ip_address ip_src,ip_address ip_dst)* function of mag.c in the MAG.

Appendix E

Software Tools and Signaling Methodology

E.1 Software Tools

The experiments carried out in chapter 5 require the use of additional software tools in the testbed. Tools were required for measuring the respective network performance parameters and to introduce background traffic in the access and core network for the purposes of emulating different network traffic behaviours. A tool was also required for introducing load in individual entities for the purposes of analysing its behaviour under varying load conditions (this tool was particularly used in the PDN-GW, and is further discussed in the packet processing delay measurement section). The following subsections provide a summary of the tools used on the testbed.

E.1.1 Wireshark protocol analyser

Wireshark [**58**] is an open-source network protocol analyser that runs on both Windows and Linux operating systems. Wireshark is a popular tool that used for network troubleshooting and analysing network traffic. It provides packet capturing capabilities using pcap [**86**] and provides a GUI interface and tools for visually displaying the traffic behaviour. The Wireshark tool is used in the testbed to measure the performance parameters in the rest of the sections.

E.1.2 Iperf

Iperf [**55**] is an open-source tool for Linux operating systems that can generate TCP or UDP streams. The streams are generated with the use of a client and server functionality provided by Iperf; the client and server functionality can be installed on any two network entities. The streams are initiated through a call from the client to the server. Iperf allows various parameters to be set for the streams like datagram size, bit-rate and a time value specifying the duration of the stream. The Iperf tool is used for generating background traffic within the testbed during the experimentation. This enables a more realistic performance evaluation to

be made.

E.1.3 Linux stress

Linux stress [**65**] is an open source workload generator utility for Linux operating systems and is used to impose certain types of stress within the hardware components of the entity running the operating system. The tool is useful for evaluating how a system would perform under varying degrees of load. The stress tool enables the introduction of artificial workers within the Central Processing Unit (CPU), Random Access Memory (RAM) or input/output ports of the network interface card that creates load within these components. The stress tool is used within the analysis of the packet processing delay in the testbed.

E.2 Signaling methodology

This section provides an overview of the signaling methodologies for the vertical handover and an IP flow handover from the LTE access network to the WLAN access network with the PMIPv6 mobility solution in the EPC, and the PMIPv6-based IP flow functionality in the EPC. The signaling methodologies do not include the access network specific signaling.

E.2.1 PMIPv6 handover from LTE to WLAN access

This section shows a call flow for a handover when a UE moves from a 3GPP Access to a non-3GPP access network. PMIPv6 used on the S5/S8 interface and the S2b interface. Figure E.1 illustrates the signaling call flow for a handover from LTE to WLAN with PMIPv6 in the EPC. The procedure is as follows;

Initial attach to E-UTRAN

1. The UE initiates the Attach procedure by transmitting to the eNodeB an Attach Request (IMSI, last visited TAI (if available), Attach Type, Selected Network, PDN Type) message. A static TAI is included in order to help the MME produce a good list of TAIs for any subsequent Attach Accept message. Selected Network indicates the E-UTRAN/LTE. PDN type indicates the requested IP version (IPv4, IPv4/IPv6, and IPv6). Attach Type indicates whether it is an EPS attach or a combined EPS/IMSI attach or an Emergency Attach.

2. The eNodeB discovers the MME and forwards the Attach Request message to the MME contained in a S1-MME control message (Initial UE message) together with the parameters obtained from the UE.

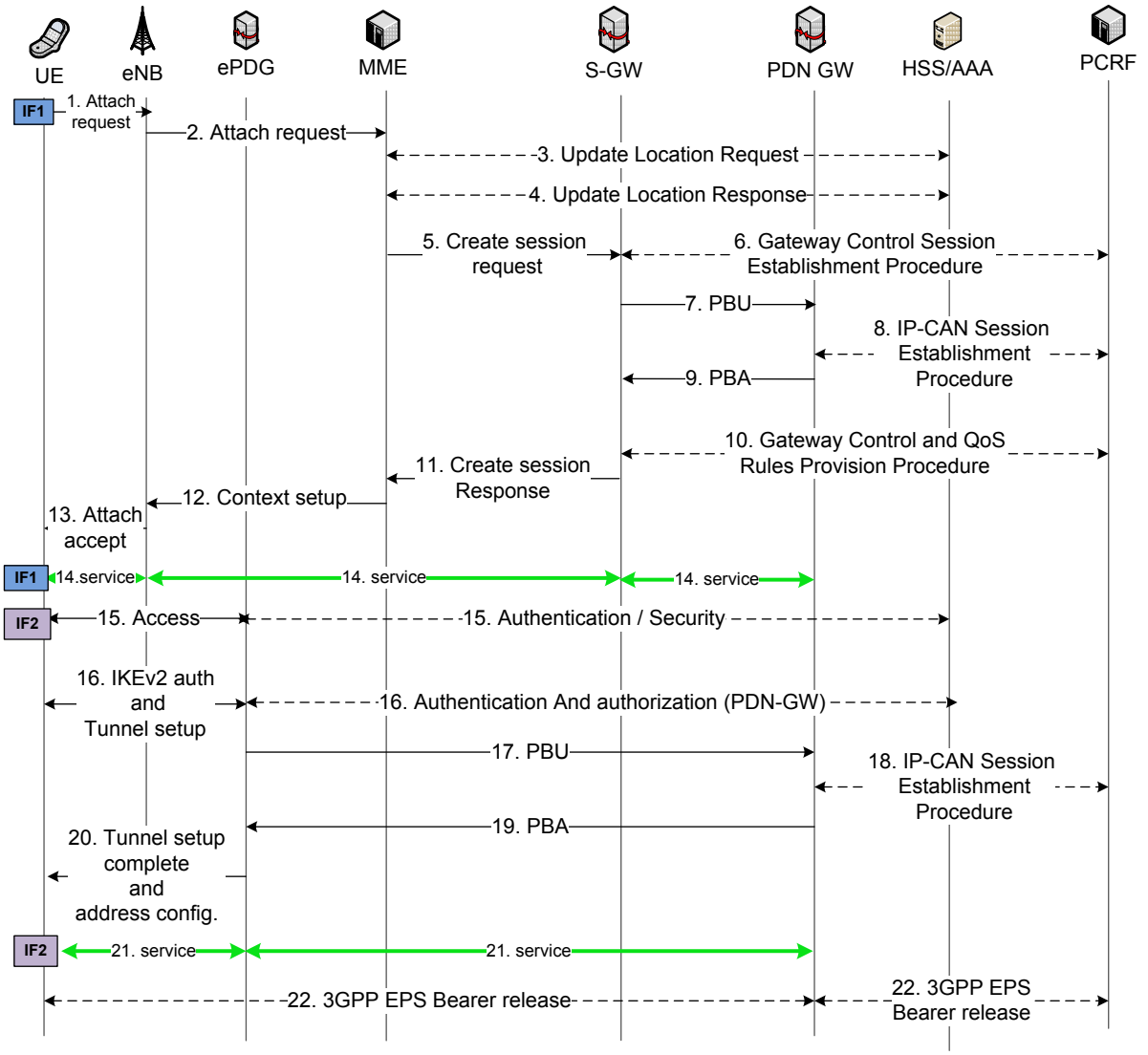

Figure E.1: Signaling methodology for the handover from LTE to WLAN with PMIPv6 in the EPC

3. The MME sends an Update Location Request (MME Identity, IMSI, ME Identity, MME Capabilities, ULR-Flags) message to the HSS. ULR-Flags indicates "Initial-Attach-Indicator" as this is an Attach procedure.

4. The HSS acknowledges the Update Location message by sending an Update Location Ack (IMSI, Subscription data) message to the new MME. The Subscription Data contain one or more PDN subscription contexts. Each PDN subscription context contains an 'EPS subscribed QoS profile. The MME then constructs a context for the UE.

5. The MME sends a Create Session Request (IMSI, MSISDN, MME TEID for control plane, PDN GW address, PDN Address, APN, RAT type, Default EPS Bearer QoS, PDN Type, EPS Bearer Identity, Handover Indication, the Protocol Type over S5/S8, Serving Network) message to the Serving GW. The Protocol Type over S5/S8 is provided to Serving GW which protocol should be used over S5/S8 interface.
6. The Serving GW initiates the Gateway Control Session Establishment Procedure with the PCRF [**11**]. The S GW provides the information to the PCRF that have been received from the MME.
7. The Serving GW sends a Proxy Binding Update (UEs IMSI, Lifetime, Access Technology Type, Handover Indicator, APN, and UE Address Info Additional Parameters) to the PDN GW in order to establish the new registration. The Lifetime field is set to a nonzero value to indicate a registration. Access Technology Type is set to indicate 3GPP access to EPS. Handover Indication option is set to indicate attachment over a new interface. The APN may be necessary to differentiate the intended PDN from the other PDNs supported by the same PDN GW. The UE Address Info IE is used to request an IPv6 prefix, IPv4 address, or both IPv4 address and IPv6 prefix and is set according to the PDN Type parameter received in the Create Session Request.
8. The PDN GW initiates the IP CAN Session Establishment Procedure with the PCRF [**11**]. The PDN GW provides information to the PCRF used to identify the session. The PDN GW also provides the PCRF with the UE IPv4 address and/or IPv6 prefix newly assigned as a result of step 7. The PCRF creates IP CAN session related information and responds to the PDN GW with PCC rules.
9. The PDN GW responds with a PMIPv6 Binding Acknowledgement (MN NAI, Lifetime, UE Address Info) message to the Serving GW. The Lifetime indicates the duration the binding will remain valid. The UE address info returns the newly assigned IPv4 address and/or IPv6 prefix assigned to the UE.
10. The PCRF initiates the Gateway Control and QoS Rules Provision Procedure [**11**] by sending a message with the QoS rules and Event Trigger information to the S GW.
11. The Serving GW returns a Create Session Response (PDN Type, PDN Address, Serving GW address for User Plane, Serving GW TEID for S1-U User Plane, Serving GW TEID for control plane, EPS Bearer Identity, EPS Bearer QoS) message to the MME.

12. The MME sends an Attach Accept (APN, PDN Type, PDN Address, TAI List, EPS Bearer Identity) message to the eNodeB.
13. The eNodeB sends the Attach Accept (APN, IP address/HNP) message to the UE. The APN is provided to the UE to notify it of the APN for which the activated default bearer is associated.
14. After the Attach Accept message, the UE can then send uplink packets towards the eNodeB which will then be tunneled to the Serving GW and PDN GW.

UE attaches and performs handover to WLAN

15. The UE attaches to a non-3GPP IP access network and performed access authentication.
16. The IKEv2 tunnel establishment procedure is started by the UE. As part of access authentication the PDN GW identity is sent to the ePDG by the 3GPP AAA server. The UE includes its address (IPv4 address or IPv6 prefix /address or both) allocated for the 3GPP Access into the during the IKEv2 message exchange to the ePDG.
17. The ePDG sends the Proxy Binding Update (IMSI, Lifetime, Access Technology Type, Handover Indicator, UE Address Info) message to the PDN GW. Access Technology Type is set to a value matching the characteristics of the non-3GPP access. The UE Address Info is set to the received IP address/HNP of step 16. The ePDG sets the handover indicator to indicate Handoff between two different interfaces of the UE.
18. The PDN GW executes a PCEF-Initiated IP CAN Session Modification Procedure with the PCRF [**11**].
19. The PDN GW processes the Proxy Binding Update message from the ePDG, updates the binding cache entry for the UE and responds with a Proxy Binding Acknowledgement (IMSI, Lifetime, UE Address Info) message. In the Proxy Binding Acknowledgement, the PDN GW replies with the same IP address and/or prefix that were assigned to the UE earlier. At this point a PMIPv6 tunnel exists between PDN GW and ePDG.
20. The ePDG and the UE continue the IKEv2 exchange and IP address configuration. At the end of the handover procedure there is a default bearer for the UE that consists of an IPsec tunnel between the UE and the ePDG and a PMIPv6 tunnel between the ePDG and the PDN GW.
21. The UEs services are then routed to the WLAN access.

22. The PDN GW shall initiate the PDN GW Initiated PDN Disconnection procedure in 3GPP access [**2**].

E.2.2 PMIPv6-based IP flow handover from LTE to WLAN access

The signaling methodology in this section only explains the steps affected by the proposed IP flow mobility enhancements. Figure E.2 illustrate the signaling methodology for an IP flow handoff from LTE to WLAN. The procedure is as follows:

Initial attach to E-UTRAN

1 - 8. Steps 1-8 of section E.2.1 above are performed. When the LMA receives the PBU message it performs the PBU message processing procedure incorporating the enhancements of Appendix D.3. Since this is the UE‟s first attach, no BCE or flow binding list exist at the LMA. Hence, the proposed enhancements in the LMA are performed but only resulting in the creation of a BCE and the allocation of a HNP to the UE. These are the standard results one would get without the proposed enhancements.

9. The LMA sends the PBA message to the S-GW (MAG) incorporating the allocated HNP to the UE. Since this is the first attach, the LMA does not add any additional HNPs to the PBA for the MAG to install. Hence, when the S-GW (MAG) receives the PBA, it performs the enhancements in section D.4 of Appendix D, but since no additional route is found during the processing of the PBA message, the MAG only creates a BULE for the allocated HNP and does not add any additional route for the UE.

10. – 13. The rest of the steps 10-13 of section E.2.1 are performed. After this the UE performs IPv6 address configuration and a tunnel and routing state (BCE, BULE) exists for the UE between t the PDN-GW and S-GW.

14. The UE can now start sending and receiving data to/from a PDN at this stage, and hence establishes two IP flows: a video streaming service and a file transfer.

Initial attach to WLAN (UE's second attach to the EPC network)

The UE is now attached to the E-UTRAN access and has discovered the WLAN access. The UE then decides to attach to WLAN access after which it requests to transfer the file tranfer to the WLAN access.

15. – 18. Steps 15-18 of section E.2.1 are performed. During these steps the UE has to provide the same APN in order for the ePDG (MAG) to select and send the PBU to the same PDN-GW used for the E-UTRAN access.

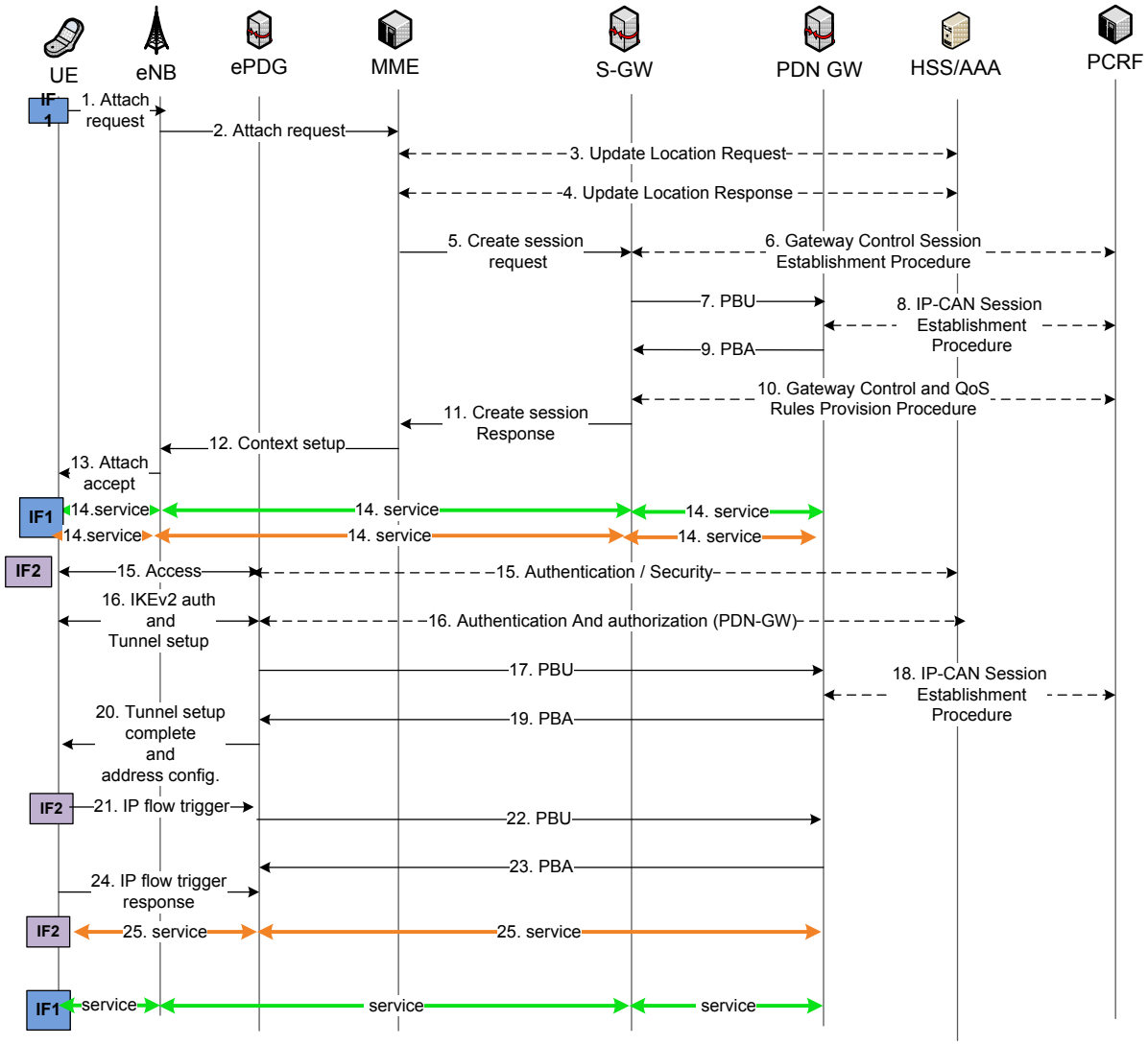

Figure E.2: Signaling methodology of an IP flow handoff from LTE to WLAN with PMIPv6 in the EPC

19. The PDN-GW (LMA), upon receiving the PBU, performs the PBU processing procedure and determines that the attach request is for an initial attach, and allocates a new HNP to the UE. Since the UE has an existing BCE, the LMA, during the PBA creation procedure, adds the previous HNP of the UE in the PBA (based on the enhancements of Appendix D.1) and sends the PBA to the ePDG (MAG). The LMA has now created two BCEs for the UE: one for the E-UTRAN access and one for the WLAN access, and each BCE having a unique HNP.

20. The ePDG (MAG), after receiving the PBA message, creates a BULE for the allocated HNP and also determines that an additional HNP was received in the PBA (based on the enhancements described in Appendix D.4), and creates an additional BULE for the UE. The ePDG (MAG) sends the new HNP (allocated by the LMA) to the UE. After these procedures a tunnel exists between the PDN-GW and ePDG for transporting the UE data traffic.

IP flow handover from E-UTRAN to WLAN

21. The UE is now attached to both the E-UTRAN and WLAN access network, and sends an IP flow mobility trigger to any of the access networks to request to create a flow binding at the PDN-GW (LMA). The IP flow mobility trigger message is not within the scope of this research, and is assumed to be an extension to the signaling messages used to perform the attach procedure to the access network. The IP flow mobility message contains the flow binding information i.e. the HNP and the routing filter. The HNP is not necessarily the HNP of the interface through which the trigger message is sent.
22. The MAG sends the flow binding information (contained in the Routing Rule mobility option) in the PBU message to the PDN-GW.
23. Upon receiving the PBU message, the LMA performs the PBU processing procedure and determines that a Routing Rule mobility option exists in the PBU (this is according to the enhancements described in Appendix D.2). The LMA then extracts the information from the PBU message and creates a flow binding list with the flow binding entry for the UE and replies with a PBA message to the MAG. The PBA contains an indication that the flow binding has been successfully created for the request. The LMA also includes any additional HNP belonging to the UE in the PBA message.
24. The MAG, after receiving the PBA message, performs the PBA message processing procedure and concludes that an additional route was received and creates a new BULE for this route (if it does not yet exist). The MAG then replies to the UE with an IP flow trigger response message containing the result of the request.
25. The UE is now receiving the file transfer IP flow through its WLAN interface.

Appendix F

Accompanying CD-ROM

The CD-ROM accompanied by this dissertation contains directories with the following files and information:

- **Research Literature** – A collection of reference papers and journals corresponding to the reference list.
- **Publications** – A collection of technical papers published by the author of this dissertation throughput the course of this research.
- **Thesis documents** – A Portable Document Format (PDF) of this dissertation and a separate copy of the dissertation abstract.
- **Thesis Software** – A collection of all the source code developed for the OpenEPC toolkit and the open source software tools used within the testbed for measurement purposes. This directory also contains detailed instructions for reconstructing the evaluation framework and evaluations.